Vulnerability Summary for the Week of December 27, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 01/04/2022 01:48 PM EST

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of December 27, 2021

01/04/2022 07:48 AM EST

Original release date: January 4, 2022

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
There were no high vulnerabilities recorded this week.				

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- log4j	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.	2021-12-28	6	CVE-2021-44832 MISC MISC MLIST CONFIRM MLIST
livehelperchat -- live_helper_chat	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-26	4.3	CVE-2021-4169 MISC CONFIRM
mediawiki -- mediawiki	In MediaWiki through 1.37, blocked IP addresses are allowed to edit EntitySchema items.	2021-12-24	5	CVE-2021-45471 MISC MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, XSS can occur in Wikibase because an external identifier property can have a URL format that includes a $1 formatter substitution marker, and the javascript: URL scheme (among others) can be used.	2021-12-24	4.3	CVE-2021-45472 MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, Wikibase item descriptions allow XSS, which is triggered upon a visit to an action=info URL (aka a page-information sidebar).	2021-12-24	4.3	CVE-2021-45473 MISC MISC
mediawiki -- mediawiki	In MediaWiki through 1.37, the Special:ImportFile URI (aka FileImporter) allows XSS, as demonstrated by the clientUrl parameter.	2021-12-24	4.3	CVE-2021-45474 MISC MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	5.2	CVE-2021-45584 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
invoiceninja -- invoice_ninja	invoiceninja is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-24	3.5	CVE-2021-3977 MISC CONFIRM

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- ac2600_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects AC2100 before 1.2.0.88, AC2400 before 1.2.0.88, AC2600 before 1.2.0.88, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.2.0.88, R6800 before 1.2.0.88, R6850 before 1.1.0.84, R6900v2 before 1.2.0.88, R7200 before 1.2.0.88, R7350 before 1.2.0.88, R7400 before 1.2.0.88, and R7450 before 1.2.0.88.	2021-12-26	not yet calculated	CVE-2021-45644 MISC
netgear -- d7000v2_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, R7000 before 1.0.11.110, R7100LG before 1.0.0.72, R7900 before 1.0.4.30, R8000 before 1.0.4.62, XR300 before 1.0.3.56, R7000P before 1.3.2.132, R8500 before 1.0.2.144, R6900P before 1.3.2.132, and R8300 before 1.0.2.144.	2021-12-26	not yet calculated	CVE-2021-45624 MISC
4nb -- videooffice	An arbitrary file download and execution vulnerability was found in the VideoOffice X2.9 and earlier versions (CVE-2020-7878). This issue is due to missing support for integrity check.	2021-12-28	not yet calculated	CVE-2020-7878 MISC
actix -- actix-web	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can unsoundly extend the lifetime of a string, leading to memory corruption.	2021-12-27	not yet calculated	CVE-2018-25025 MISC MISC
actix -- actix-web	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can unsoundly coerce an immutable reference into a mutable reference, leading to memory corruption.	2021-12-27	not yet calculated	CVE-2018-25024 MISC MISC
actix -- actix-web	An issue was discovered in the actix-web crate before 0.7.15 for Rust. It can add the Send marker trait to an object that cannot be sent between threads safely, leading to memory corruption.	2021-12-27	not yet calculated	CVE-2018-25026 MISC MISC
apache -- apisix_dashboard	In Apache APISIX Dashboard before 2.10.1, the Manager API uses two frameworks and introduces framework `droplet` on the basis of framework `gin`, all APIs and authentication middleware are developed based on framework `droplet`, but some API directly use the interface of framework `gin` thus bypassing the authentication.	2021-12-27	not yet calculated	CVE-2021-45232 CONFIRM MLIST
archivy -- archivy	archivy is vulnerable to Cross-Site Request Forgery (CSRF)	2021-12-25	not yet calculated	CVE-2021-4162 CONFIRM MISC
asus -- rt-n53_devices	ASUS RT-N53 3.0.0.4.376.3754 devices have a buffer overflow via a long lan_dns1_x or lan_dns2_x parameter to Advanced_LAN_Content.asp.	2021-12-28	not yet calculated	CVE-2019-20082 MISC MISC
attendance_management_system -- attendance_management_system	Attendance Management System 1.0 is affected by a Cross Site Scripting (XSS) vulnerability. The value of the FirstRecord request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The attacker can access the system, by using the XSS-reflected method, and then can store information by injecting the admin account on this system.	2021-12-26	not yet calculated	CVE-2021-44598 MISC
authguard -- authguard	basic/BasicAuthProvider.java in AuthGuard before 0.9.0 allows authentication via an inactive identifier.	2021-12-27	not yet calculated	CVE-2021-45890 MISC MISC MISC MISC
avast -- antivirus	Privilege escalation vulnerability in Avast Antivirus prior to 20.4 allows a local user to gain elevated privileges by "hollowing" trusted process which could lead to the bypassing of Avast self-defense.	2021-12-27	not yet calculated	CVE-2021-45339 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
avast -- antivirus	Privilege escalation vulnerability in the Sandbox component of Avast Antivirus prior to 20.4 allows a local sandboxed code to gain elevated privileges by using system IPC interfaces which could lead to exit the sandbox and acquire SYSTEM privileges.	2021-12-27	not yet calculated	CVE-2021-45336 MISC MISC
avast -- antivirus	Privilege escalation vulnerability in the Self-Defense driver of Avast Antivirus prior to 20.8 allows a local user with SYSTEM privileges to gain elevated privileges by "hollowing" process wsc_proxy.exe which could lead to acquire antimalware (AM-PPL) protection.	2021-12-27	not yet calculated	CVE-2021-45337 MISC MISC
avast -- antivirus	Multiple privilege escalation vulnerabilities in Avast Antivirus prior to 20.4 allow a local user to gain elevated privileges by calling unnecessarily powerful internal methods of the main antivirus service which could lead to the (1) arbitrary file delete, (2) write and (3) reset security.	2021-12-27	not yet calculated	CVE-2021-45338 MISC MISC MISC MISC
avast -- antivirus	Sandbox component in Avast Antivirus prior to 20.4 has an insecure permission which could be abused by local user to control the outcome of scans, and therefore evade detection or delete arbitrary system files.	2021-12-27	not yet calculated	CVE-2021-45335 MISC MISC
biostar -- racing_gt_evo	An issue was discovered in BS_RCIO64.sys in Biostar RACING GT Evo 2.1.1905.1700. A low-integrity process can open the driver's device object and issue IOCTLs to read or write to arbitrary physical memory locations (or call an arbitrary address), leading to execution of arbitrary code. This is associated with 0x226040, 0x226044, and 0x226000.	2022-01-01	not yet calculated	CVE-2021-44852 MISC
bitmask -- riseup	Bitmask Riseup VPN 0.21.6 contains a local privilege escalation flaw due to improper access controls. When the software is installed with a non-default installation directory off of the system root, the installer fails to properly set ACLs. This allows lower privileged users to replace the VPN executable with a malicious one. When a higher privileged user such as an Administrator launches that executable, it is possible for the lower privileged user to escalate to Administrator privileges.	2021-12-30	not yet calculated	CVE-2021-44466 MISC
brave -- brave_desktop	In Brave Desktop 1.17 through 1.33 before 1.33.106, when CNAME-based adblocking and a proxying extension with a SOCKS fallback are enabled, additional DNS requests are issued outside of the proxying extension using the system's DNS settings, resulting in information disclosure. NOTE: this issue exists because of an incomplete fix for CVE-2021-21323 and CVE-2021-22916.	2021-12-27	not yet calculated	CVE-2021-45884 MISC MISC MISC MISC
carinal -- tien_hospital_health_report_system	Carinal Tien Hospital Health Report System's login page has improper authentication, a remote attacker can acquire another general user's privilege by modifying the cookie parameter without authentication. The attacker can then perform limited operations on the system or modify data, making the service partially unavailable to the user.	2021-12-29	not yet calculated	CVE-2021-44160 MISC
celery -- celery	This affects the package celery before 5.2.2. It by default trusts the messages and metadata stored in backends (result stores). When reading task metadata from the backend, the data is deserialized. Given that an attacker can gain access to, or somehow manipulate the metadata within a celery backend, they could trigger a stored command injection vulnerability and potentially gain further access to the system.	2021-12-29	not yet calculated	CVE-2021-23727 MISC MISC
cscms -- cscms	An issue in the user login box of CSCMS v4.0 allows attackers to hijack user accounts via brute force attacks.	2021-12-27	not yet calculated	CVE-2020-21238 MISC
damicms -- damicms	A vulnerability in /damicms-master/admin.php?s=/Article/doedit of DamiCMS v6.0 allows attackers to compromise and impersonate user accounts via obtaining a user's session cookie.	2021-12-27	not yet calculated	CVE-2020-21236 MISC
dl-axist -- devices	The Datalogic DXU service on (for example) DL-Axist devices does not require authentication for configuration changes or disclosure of configuration settings.	2022-01-01	not yet calculated	CVE-2021-43333 MISC CONFIRM
dmp -- roadmap	DMP Roadmap before 3.0.4 allows XSS.	2022-01-01	not yet calculated	CVE-2021-44896 MISC MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in answer_request (called from FuzzAnswerTheRequest and fuzz_rfc1035.c).	2022-01-01	not yet calculated	CVE-2021-45957 MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in check_bad_address (called from check_for_bogus_wildcard and FuzzCheckForBogusWildcard).	2022-01-01	not yet calculated	CVE-2021-45951 MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in print_mac (called from log_packet and dhcp_reply).	2022-01-01	not yet calculated	CVE-2021-45956 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in dhcp_reply (called from dhcp_packet and FuzzDhcp).	2022-01-01	not yet calculated	CVE-2021-45952 MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from hash_questions and fuzz_util.c).	2022-01-01	not yet calculated	CVE-2021-45953 MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in extract_name (called from answer_auth and FuzzAuth).	2022-01-01	not yet calculated	CVE-2021-45954 MISC MISC
dnsmasq -- dnsmasq	Dnsmasq 2.86 has a heap-based buffer overflow in resize_packet (called from FuzzResizePacket and fuzz_rfc1035.c).	2022-01-01	not yet calculated	CVE-2021-45955 MISC MISC
elgg -- elgg	elgg is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-24	not yet calculated	CVE-2021-4072 MISC CONFIRM
emerson -- xweb_300d_evo	Emerson XWEB 300D EVO 3.0.7--3ee403 is affected by: unauthenticated arbitrary file deletion due to path traversal. An attacker can browse and delete files without any authentication due to incorrect access control and directory traversal.	2021-12-30	not yet calculated	CVE-2021-45427 MISC MISC MISC
emuse -- eservices_and_envoice	Emuse - eServices / eNvoice SQL injection can be used in various ways ranging from bypassing login authentication or dumping the whole database to full RCE on the affected endpoints. The SQLi caused by CWE-209: Generation of Error Message Containig Sensetive Information, showing parts of the aspx code and the webroot location , information an attacker can leverage to further compromise the host.	2021-12-29	not yet calculated	CVE-2021-36722 CONFIRM
emuse -- eservices_and_envoice	Emuse - eServices / eNvoice Exposure Of Private Personal Information due to lack of identification mechanisms and predictable IDs an attacker can scrape all the files on the service.	2021-12-29	not yet calculated	CVE-2021-36723 CONFIRM
evga -- precision_xoc	The WinRin0x64.sys and WinRing0.sys low-level drivers in EVGA Precision XOC version v6.2.7 were discovered to be configured with the default security descriptor which allows attackers to access sensitive components and data.	2021-12-28	not yet calculated	CVE-2020-22057 MISC
expat -- expat	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).	2022-01-01	not yet calculated	CVE-2021-45960 MISC MISC MISC
fatek -- winproladder	FATEK WinProladder Versions 3.30_24518 and prior are vulnerable to a stack-based buffer overflow while processing project files, which may allow an attacker to execute arbitrary code.	2021-12-28	not yet calculated	CVE-2021-43556 MISC
fatek -- winproladder	FATEK WinProladder Versions 3.30_24518 and prior are vulnerable to an out-of-bounds write while processing project files, which may allow an attacker to execute arbitrary code.	2021-12-28	not yet calculated	CVE-2021-43554 MISC
forescout -- secureconnector_local_service	ForeScout - SecureConnector Local Service DoS - A low privilaged user which doesn't have permissions to shutdown the secure connector service writes a large amount of characters in the installationPath. This will cause the buffer to overflow and override the stack cookie causing the service to crash.	2021-12-29	not yet calculated	CVE-2021-36724 CONFIRM
gdal -- gdal	GDAL 3.3.0 through 3.4.0 has a heap-based buffer overflow in PCIDSK::CPCIDSKFile::ReadFromFile (called from PCIDSK::CPCIDSKSegment::ReadFromFile and PCIDSK::CPCIDSKBinarySegment::CPCIDSKBinarySegment).	2022-01-01	not yet calculated	CVE-2021-45943 MISC MISC MISC MISC
gerapy -- gerapy	Gerapy is a distributed crawler management framework. Gerapy prior to version 0.9.8 is vulnerable to remote code execution, and this issue is patched in version 0.9.8.	2021-12-27	not yet calculated	CVE-2021-43857 CONFIRM MISC MISC
ghostscript -- ghostpdl	Ghostscript GhostPDL 9.50 through 9.53.3 has a use-after-free in sampled_data_sample (called from sampled_data_continue and interp).	2022-01-01	not yet calculated	CVE-2021-45944 MISC MISC
ghostscript -- ghostpdl	Ghostscript GhostPDL 9.50 through 9.54.0 has a heap-based buffer overflow in sampled_data_finish (called from sampled_data_continue and interp).	2022-01-01	not yet calculated	CVE-2021-45949 MISC MISC MISC
gif2apng -- gif2apng	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow within the main function. It allows an attacker to write data outside of the allocated buffer. The attacker has control over a part of the address that data is written to, control over the written data, and (to some extent) control over the amount of data that is written.	2021-12-28	not yet calculated	CVE-2021-45910 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gif2apng -- gif2apng	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow vulnerability in the DecodeLZW function. It allows an attacker to write a large amount of arbitrary data outside the boundaries of a buffer.	2021-12-28	not yet calculated	CVE-2021-45909 MISC
gif2apng -- gif2apng	An issue was discovered in gif2apng 1.9. There is a stack-based buffer overflow involving a for loop. An attacker has little influence over the data written to the stack, making it unlikely that the flow of control can be subverted.	2021-12-28	not yet calculated	CVE-2021-45907 MISC
gif2apng -- gif2apng	An issue was discovered in gif2apng 1.9. There is a stack-based buffer overflow involving a while loop. An attacker has little influence over the data written to the stack, making it unlikely that the flow of control can be subverted.	2021-12-28	not yet calculated	CVE-2021-45908 MISC
gif2apng -- gif2apng	An issue was discovered in gif2apng 1.9. There is a heap-based buffer overflow in the main function. It allows an attacker to write 2 bytes outside the boundaries of the buffer.	2021-12-28	not yet calculated	CVE-2021-45911 MISC
giftrans -- giftrans	The giftrans function in giftrans 1.12.2 contains a stack-based buffer overflow because a value inside the input file determines the amount of data to write. This allows an attacker to overwrite up to 250 bytes outside of the allocated buffer with arbitrary data.	2022-01-01	not yet calculated	CVE-2021-45972 MISC MISC MISC
glewlwyd -- glewlwyd	Glewlwyd 2.0.0, fixed in 2.6.1 is affected by an incorrect access control vulnerability. One user can attempt to log in as another user without its password.	2021-12-30	not yet calculated	CVE-2021-45379 MISC MISC
go -- go	net/http in Go before 1.16.12 and 1.17.x before 1.17.5 allows uncontrolled memory consumption in the header canonicalization cache via HTTP/2 requests.	2022-01-01	not yet calculated	CVE-2021-44716 CONFIRM
go -- go	Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network connection as a consequence of erroneous closing of file descriptor 0 after file-descriptor exhaustion.	2022-01-01	not yet calculated	CVE-2021-44717 CONFIRM
google -- android	An improper authentication vulnerability has been reported to affect Android App Qfile. If exploited, this vulnerability allows attackers to compromise app and access information We have already fixed this vulnerability in the following versions of Qfile: Qfile 3.0.0.1105 and later	2021-12-29	not yet calculated	CVE-2021-38688 CONFIRM
grok -- grok	Grok 9.5.0 has a heap-based buffer overflow in openhtj2k::T1OpenHTJ2K::decompress (called from std::__1::__packaged_task_func<std::__1::__bind<grk::T1DecompressScheduler::dead and std::__1::packaged_task<int>).	2022-01-01	not yet calculated	CVE-2021-45935 MISC MISC MISC
groupsession -- bycloud_and_zion	Path traversal vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows an attacker with an administrative privilege to obtain sensitive information stored in the hierarchy above the directory on the published site's server via unspecified vectors.	2021-12-24	not yet calculated	CVE-2021-20876 MISC MISC
groupsession -- bycloud_and_zion	Incorrect permission assignment for critical resource vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to access arbitrary files on the server and obtain sensitive information via unspecified vectors.	2021-12-24	not yet calculated	CVE-2021-20874 MISC MISC
groupsession -- bycloud_and_zion	Open redirect vulnerability in GroupSession Free edition ver5.1.1 and earlier, GroupSession byCloud ver5.1.1 and earlier, and GroupSession ZION ver5.1.1 and earlier allows a remote unauthenticated attacker to redirect users to arbitrary web sites and conduct phishing attacks by having a user to access a specially crafted URL.	2021-12-24	not yet calculated	CVE-2021-20875 MISC MISC
harfbuzz-- harfbuzz	HarfBuzz 2.9.0 has an out-of-bounds write in hb_bit_set_invertible_t::set (called from hb_sparseset_t<hb_bit_set_invertible_t>::set and hb_set_copy).	2022-01-01	not yet calculated	CVE-2021-45931 MISC MISC MISC
iball -- wrd12en	iBall WRD12EN 1.0.0 devices allow cross-site request forgery (CSRF) attacks as demonstrated by enabling DNS settings or modifying the range for IP addresses.	2021-12-30	not yet calculated	CVE-2020-29292 MISC MISC
ibm -- x-force	IBM OPENBMC OP910 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 212049.	2021-12-27	not yet calculated	CVE-2021-38961 CONFIRM XF
ibm -- x-force	IBM i 7.2, 7.3, and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 208404.	2021-12-30	not yet calculated	CVE-2021-38876 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
idec -- idec	Unprotected transport of credentials vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from the communication between the PLC and the software. As a result, the complete access privileges to the PLC Web server may be obtained, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	2021-12-24	not yet calculated	CVE-2021-20826 MISC MISC
idec -- idec	Plaintext storage of a password vulnerability in IDEC PLCs (FC6A Series MICROSmart All-in-One CPU module v2.32 and earlier, FC6A Series MICROSmart Plus CPU module v1.91 and earlier, WindLDR v8.19.1 and earlier, WindEDIT Lite v1.3.1 and earlier, and Data File Manager v2.12.1 and earlier) allows an attacker to obtain the PLC Web server user credentials from file servers, backup repositories, or ZLD files saved in SD cards. As a result, the attacker may access the PLC Web server and hijack the PLC, and manipulation of the PLC output and/or suspension of the PLC may be conducted.	2021-12-24	not yet calculated	CVE-2021-20827 MISC MISC
idec -- multiple_products	An attacker may obtain the user credentials from file servers, backup repositories, or ZLD files saved in SD cards. As a result, the PLC user program may be uploaded, altered, and/or downloaded.	2021-12-28	not yet calculated	CVE-2021-37401 MISC MISC MISC MISC
idec -- multiple_products	An attacker may obtain the user credentials from the communication between the PLC and the software. As a result, the PLC user program may be uploaded, altered, and/or downloaded.	2021-12-28	not yet calculated	CVE-2021-37400 MISC MISC MISC MISC
ifme -- ifme	In “ifme”, versions 1.0.0 to v7.31.4 are vulnerable against stored XSS vulnerability in the markdown editor. It can be exploited by making a victim a Leader of a group which triggers the payload for them.	2021-12-29	not yet calculated	CVE-2021-25989 MISC CONFIRM
ifme -- ifme	In “ifme”, versions v7.22.0 to v7.31.4 are vulnerable against self-stored XSS in the contacts field as it allows loading XSS payloads fetched via an iframe.	2021-12-29	not yet calculated	CVE-2021-25990 MISC CONFIRM
ifme -- ifme	In Ifme, versions v5.0.0 to v7.32 are vulnerable against an improper access control, which makes it possible for admins to ban themselves leading to their deactivation from Ifme account and complete loss of admin access to Ifme.	2021-12-29	not yet calculated	CVE-2021-25991 MISC CONFIRM
ifme -- ifme	In “ifme”, versions 1.0.0 to v7.31.4 are vulnerable against stored XSS vulnerability (notifications section) which can be directly triggered by sending an ally request to the admin.	2021-12-29	not yet calculated	CVE-2021-25988 CONFIRM MISC
intellibridge -- ec_40_and_60_hub	The standard access path of the IntelliBridge EC 40 and 60 Hub (C.00.04 and prior) requires authentication, but the product has an alternate path or channel that does not require authentication.	2021-12-27	not yet calculated	CVE-2021-33017 MISC
intellibridge -- ec_40_and_60_hub	IntelliBridge EC 40 and 60 Hub (C.00.04 and prior) contains hard-coded credentials, such as a password or a cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2021-12-27	not yet calculated	CVE-2021-32993 MISC
iris -- iris	This affects all versions of package github.com/kataras/iris; all versions of package github.com/kataras/iris/v12. The unsafe handling of file names during upload using UploadFormFiles method may enable attackers to write to arbitrary locations outside the designated target folder.	2021-12-24	not yet calculated	CVE-2021-23772 CONFIRM CONFIRM CONFIRM
jeecg -- jeecg	An arbitrary file download vulnerability in jeecg v3.8 allows attackers to access sensitive files via modification of the "localPath" variable.	2021-12-27	not yet calculated	CVE-2020-20948 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jquery -- terminal_emulator	jQuery Terminal Emulator is a plugin for creating command line interpreters in your applications. Versions prior to 2.31.1 contain a low impact and limited cross-site scripting (XSS) vulnerability. The code for XSS payload is always visible, but an attacker can use other techniques to hide the code the victim sees. If the application uses the `execHash` option and executes code from URL, the attacker can use this URL to execute their code. The scope is limited because the javascript attribute used is added to span tag, so no automatic execution like with `onerror` on images is possible. This issue is fixed in version 2.31.1. As a workaround, the user can use formatting that wrap whole user input and its no op. The code for this workaround is available in the GitHub Security Advisory. The fix will only work when user of the library is not using different formatters (e.g. to highlight code in different way).	2021-12-30	not yet calculated	CVE-2021-43862 CONFIRM MISC MISC MISC
js-data -- js-data	All versions of package js-data are vulnerable to Prototype Pollution via the deepFillIn and the set functions. This is an incomplete fix of [CVE-2020-28442](https://snyk.io/vuln/SNYK-JS-JSDATA-1023655).	2021-12-24	not yet calculated	CVE-2021-23574 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
kubernetes -- minio	MinIO is a Kubernetes native application for cloud storage. Prior to version `RELEASE.2021-12-27T07-23-18Z`, a malicious client can hand-craft an HTTP API call that allows for updating policy for a user and gaining higher privileges. The patch in version `RELEASE.2021-12-27T07-23-18Z` changes the accepted request body type and removes the ability to apply policy changes through this API. There is a workaround for this vulnerability: Changing passwords can be disabled by adding an explicit `Deny` rule to disable the API for users.	2021-12-27	not yet calculated	CVE-2021-43858 MISC MISC MISC CONFIRM MISC
libbpf -- libbpf	libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (8 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).	2022-01-01	not yet calculated	CVE-2021-45941 MISC MISC
libbpf -- libbpf	libbpf 0.6.0 and 0.6.1 has a heap-based buffer overflow (4 bytes) in __bpf_object__open (called from bpf_object__open_mem and bpf-object-fuzzer.c).	2022-01-01	not yet calculated	CVE-2021-45940 MISC MISC
libjxl -- libjxl	libjxl b02d6b9, as used in libvips 8.11 through 8.11.2 and other products, has an out-of-bounds write in jxl::ModularFrameDecoder::DecodeGroup (called from jxl::FrameDecoder::ProcessACGroup and jxl::ThreadPool::RunCallState<jxl::FrameDecoder::ProcessSections).	2022-01-01	not yet calculated	CVE-2021-45928 MISC MISC MISC MISC MISC
libredwg -- libredwg	LibreDWG 0.12.4.4313 through 0.12.4.4367 has an out-of-bounds write in dwg_free_BLOCK_private (called from dwg_free_BLOCK and dwg_free_object).	2022-01-01	not yet calculated	CVE-2021-45950 MISC MISC
linux -- linux_kernel	In the IPv6 implementation in the Linux kernel before 5.13.3, net/ipv6/output_core.c has an information leak because of certain use of a hash table which, although big, doesn't properly consider that IPv6-based attackers can typically choose among many IPv6 source addresses.	2021-12-25	not yet calculated	CVE-2021-45485 MISC MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.15.11. There is a memory leak in the __rds_conn_create() function in net/rds/connection.c in a certain combination of circumstances.	2021-12-24	not yet calculated	CVE-2021-45480 MISC MISC
linux -- linux_kernel	In the IPv4 implementation in the Linux kernel before 5.12.4, net/ipv4/route.c has an information leak because the hash table is very small.	2021-12-25	not yet calculated	CVE-2021-45486 MISC MISC MISC
livehelperchat -- livehelperchat	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-29	not yet calculated	CVE-2021-4175 MISC CONFIRM
livehelperchat -- livehelperchat	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-29	not yet calculated	CVE-2021-4176 CONFIRM MISC
livehelperchat -- livehelperchat	livehelperchat is vulnerable to Generation of Error Message Containing Sensitive Information	2021-12-28	not yet calculated	CVE-2021-4177 MISC CONFIRM
livehelperchat -- livehelperchat	livehelperchat is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2021-12-28	not yet calculated	CVE-2021-4179 MISC CONFIRM
ljcms -- ljcms	An issue in the user login box of LJCMS v1.11 allows attackers to hijack user accounts via brute force attacks.	2021-12-27	not yet calculated	CVE-2020-21237 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
max_mazurov -- maddy	A Broken or Risky Cryptographic Algorithm exists in Max Mazurov Maddy before 0.5.2, which is an unnecessary risk that may result in the exposure of sensitive information.	2021-12-28	not yet calculated	CVE-2021-42583 MISC MISC
mdbtools -- mdbtools	MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd0c689be0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).	2022-01-01	not yet calculated	CVE-2021-45926 MISC MISC MISC
mdbtools -- mdbtools	MDB Tools (aka mdbtools) 0.9.2 has a stack-based buffer overflow (at 0x7ffd6e029ee0) in mdb_numeric_to_string (called from mdb_xfer_bound_data and _mdb_attempt_bind).	2022-01-01	not yet calculated	CVE-2021-45927 MISC MISC MISC
mermaid -- mermaid	Mermaid is a Javascript based diagramming and charting tool that uses Markdown-inspired text definitions and a renderer to create and modify complex diagrams. Prior to version 8.13.8, malicious diagrams can run javascript code at diagram readers' machines. Users should upgrade to version 8.13.8 to receive a patch. There are no known workarounds aside from upgrading.	2021-12-30	not yet calculated	CVE-2021-43861 MISC MISC CONFIRM
microsoft -- sharepoint	Microsoft SharePoint Elevation of Privilege Vulnerability.	2021-12-29	not yet calculated	CVE-2021-43876 MISC
motp -- motp	Changing MOTP (Mobile One Time Password) system's specific function parameter has insufficient validation for user input. A attacker in local area network can perform SQL injection attack to read, modify or delete backend database without authentication.	2021-12-29	not yet calculated	CVE-2021-44161 MISC
moxa -- multiple_mgate_products	The affected products contain vulnerable firmware, which could allow an attacker to sniff the traffic and decrypt login credential details. This could give an attacker admin rights through the HTTP web server.	2021-12-27	not yet calculated	CVE-2021-4161 MISC
mruby -- mruby	mruby is vulnerable to NULL Pointer Dereference	2021-12-30	not yet calculated	CVE-2021-4188 MISC CONFIRM
netbsd -- netbsd	In NetBSD through 9.2, the IPv4 ID generation algorithm does not use appropriate cryptographic measures.	2021-12-25	not yet calculated	CVE-2021-45487 MISC MISC
netbsd -- netbsd	In NetBSD through 9.2, the IPv6 fragment ID generation algorithm employs a weak cryptographic PRNG.	2021-12-25	not yet calculated	CVE-2021-45484 MISC MISC
netbsd -- netbsd	In NetBSD through 9.2, the IPv6 Flow Label generation algorithm employs a weak cryptographic PRNG.	2021-12-25	not yet calculated	CVE-2021-45489 MISC MISC
netbsd -- netbsd	In NetBSD through 9.2, there is an information leak in the TCP ISN (ISS) generation algorithm.	2021-12-25	not yet calculated	CVE-2021-45488 MISC MISC
netgear -- ac2100_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects AC2100 before 1.2.0.88, AC2400 before 1.2.0.88, AC2600 before 1.2.0.88, D7000 before 1.0.1.82, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.2.0.88, R6800 before 1.2.0.88, R6850 before 1.1.0.84, R6900v2 before 1.2.0.88, R7200 before 1.2.0.88, R7350 before 1.2.0.88, R7400 before 1.2.0.88, and R7450 before 1.2.0.88.	2021-12-26	not yet calculated	CVE-2021-45534 MISC MISC
netgear -- ac2100_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects AC2100 before 2021-08-27, AC2400 before 2021-08-27, AC2600 before 2021-08-27, D7000 before 2021-08-27, R6220 before 2021-08-27, R6230 before 2021-08-27, R6260 before 2021-08-27, R6330 before 2021-08-27, R6350 before 2021-08-27, R6700v2 before 2021-08-27, R6800 before 2021-08-27, R6850 before 2021-08-27, R6900v2 before 2021-08-27, R7200 before 2021-08-27, R7350 before 2021-08-27, R7400 before 2021-08-27, and R7450 before 2021-08-27.	2021-12-26	not yet calculated	CVE-2021-45511 MISC
netgear -- ac2400_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects AC2400 before 1.1.0.84, AC2600 before 1.1.0.84, D7000 before 1.0.1.82, R6020 before 1.0.0.52, R6080 before 1.0.0.52, R6120 before 1.0.0.80, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.84, R6330 before 1.1.0.84, R6350 before 1.1.0.84, R6700v2 before 1.1.0.84, R6800 before 1.1.0.84, R6850 before 1.1.0.84, R6900v2 before 1.1.0.84, R7200 before 1.1.0.84, R7350 before 1.1.0.84, R7400 before 1.1.0.84, and R7450 before 1.1.0.84.	2021-12-26	not yet calculated	CVE-2021-45501 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX7500 before 1.0.0.72, R6400 before 1.0.1.68, R6900P before 1.3.2.132, R7000 before 1.0.11.116, R7000P before 1.3.2.132, R7900 before 1.0.4.38, R7960P before 1.4.1.66, R8000 before 1.0.4.66, RAX200 before 1.0.3.106, RS400 before 1.5.1.80, XR300 before 1.0.3.68, MK62 before 1.0.6.110, MR60 before 1.0.6.110, R6400v2 before 1.0.4.106, R8000P before 1.4.1.66, RAX20 before 1.0.2.64, RAX45 before 1.0.2.82, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, R6700v3 before 1.0.4.106, R7900P before 1.4.1.66, RAX15 before 1.0.2.64, RAX50 before 1.0.2.82, RAX75 before 1.0.3.106, RBR750 before 3.2.16.22, RBR850 before 3.2.16.22, RBS750 before 3.2.16.22, RBS850 before 3.2.16.22, RBK752 before 3.2.16.22, and RBK852 before 3.2.16.22.	2021-12-26	not yet calculated	CVE-2021-45617 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45598 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45597 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by reflected XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.32, EAX80 before 1.0.1.62, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7000 before 1.0.1.104, EX7500 before 1.0.0.72, R7000 before 1.0.11.110, R7900 before 1.0.4.30, R7960P before 1.4.1.66, R8000 before 1.0.4.62, RAX200 before 1.0.2.102, XR300 before 1.0.3.50, EX3700 before 1.0.0.90, MR60 before 1.0.5.102, R7000P before 1.3.2.126, R8000P before 1.4.1.66, RAX20 before 1.0.1.64, RAX50 before 1.0.2.28, RAX80 before 1.0.3.102, EX3800 before 1.0.0.90, MS60 before 1.0.5.102, R6900P before 1.3.2.126, R7900P before 1.4.1.66, RAX15 before 1.0.1.64, RAX45 before 1.0.2.28, RAX75 before 1.0.3.102, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45639 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000P before 1.4.2.84, R8300 before 1.0.2.154, R8500 before 1.0.2.154, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45615 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6400 before 1.0.1.70, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	2021-12-26	not yet calculated	CVE-2021-45622 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7960P before 1.4.1.66, RAX200 before 1.0.3.106, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, EX3700 before 1.0.0.90, MR60 before 1.0.6.110, R8000P before 1.4.1.66, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, EX3800 before 1.0.0.90, MS60 before 1.0.6.110, R7900P before 1.4.1.66, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45667 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 3.2.18.2, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBS40V before 2.6.2.4, and RBW30 before 2.6.2.2.	2021-12-26	not yet calculated	CVE-2021-45628 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45631 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45630 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	2021-12-26	not yet calculated	CVE-2021-45612 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX80 before 1.0.1.62, EX7500 before 1.0.0.72, R7900 before 1.0.4.38, R8000 before 1.0.4.68, RAX200 before 1.0.4.120, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.4.120, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.4.120, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45671 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, D7000v2 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, MR80 before 1.1.2.20, MS80 before 1.1.2.20, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX43 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX35v2 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45613 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, LAX20 before 1.1.6.28, MR60 before 1.0.6.116, MR80 before 1.1.2.20, MS60 before 1.0.6.116, MS80 before 1.1.2.20, MK62 before 1.0.6.116, MK83 before 1.1.2.20, R6400 before 1.0.1.70, R6400v2 before 1.0.4.106, R6700v3 before 1.0.4.106, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	2021-12-26	not yet calculated	CVE-2021-45620 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects CBR40 before 2.3.5.12, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, R6400 before 1.0.1.70, R7000 before 1.0.11.126, R6900P before 1.3.2.124, R7000P before 1.3.2.124, R7900 before 1.0.4.30, R8000 before 1.0.4.52, and WNR3500Lv2 before 1.2.0.62.	2021-12-26	not yet calculated	CVE-2021-45529 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBW30 before 2.6.2.2, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBS40V before 2.6.2.8.	2021-12-26	not yet calculated	CVE-2021-45507 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX80 before 1.0.1.64, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, RBW30 before 2.6.1.4, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, and RBS40V before 2.6.1.4.	2021-12-26	not yet calculated	CVE-2021-45666 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.24, CBR750 before 3.2.18.2, EAX20 before 1.0.0.58, EAX80 before 1.0.1.68, EX3700 before 1.0.0.94, EX3800 before 1.0.0.94, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7000 before 1.0.1.104, EX7500 before 1.0.0.74, LAX20 before 1.1.6.28, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6300v2 before 1.0.4.52, R6400 before 1.0.1.70, R6400v2 before 1.0.4.106, R6700v3 before 1.0.4.106, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7100LG before 1.0.0.72, R7850 before 1.0.5.74, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, R8300 before 1.0.2.154, R8500 before 1.0.2.154, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, XR1000 before 1.0.0.58, and XR300 before 1.0.3.68.	2021-12-26	not yet calculated	CVE-2021-45621 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBR852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45504 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by stored XSS. This affects CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7000 before 1.0.11.116, R7900 before 1.0.4.38, R8000 before 1.0.4.68, RAX200 before 1.0.3.106, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, EX3700 before 1.0.0.90, MR60 before 1.0.6.110, R7000P before 1.3.2.126, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, EX3800 before 1.0.0.90, MS60 before 1.0.6.110, R6900P before 1.3.2.126, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45670 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, and RBR850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45508 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR40 before 2.5.0.24, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45509 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45601 MISC
netgear -- cbr40_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR40 before 2.5.0.24, CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45599 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45627 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR750 before 4.6.3.6, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45600 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45506 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45503 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45633 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects CBR750 before 3.2.18.2, D6220 before 1.0.0.68, D6400 before 1.0.0.102, D8500 before 1.0.3.60, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6300v2 before 1.0.4.50, R6400 before 1.0.1.68, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45604 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45505 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45596 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45502 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45632 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45634 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45635 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 3.2.18.2, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45616 MISC
netgear -- cbr750_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR750 before 4.6.3.6, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45629 MISC
netgear -- d3600_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.78, D6100 before 1.0.0.63, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DGN2200Bv4 before 1.0.0.109, DGN2200v4 before 1.0.0.110, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v3 before 1.0.2.66, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R7000 before 1.0.9.42, R7000P before 1.3.1.64, R7100LG before 1.0.0.50, R7300 before 1.0.0.70, R7900 before 1.0.3.8, R7900P before 1.4.1.30, R8000 before 1.0.4.28, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, WNDR3400v3 before 1.0.1.24, WNR3500Lv2 before 1.2.0.62, and XR500 before 2.3.2.56.	2021-12-26	not yet calculated	CVE-2021-45550 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- d3600_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, D6200 before 1.1.00.34, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000 before 1.0.1.74, D7000v2 before 1.0.0.53, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DC112A before 1.0.0.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, DM200 before 1.0.0.61, EX3700 before 1.0.0.76, EX3800 before 1.0.0.76, EX6120 before 1.0.0.46, EX6130 before 1.0.0.28, EX7000 before 1.0.1.78, PR2000 before 1.0.0.28, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v3 before 1.0.2.66, R6900 before 1.0.2.6, R7000 before 1.0.9.34, R7100LG before 1.0.0.50, R7500v2 before 1.0.3.40, R7900P before 1.4.1.50, R8000P before 1.4.1.50, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBK40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR20 before 2.3.0.28, RBR40 before 2.3.0.28, RBR50 before 2.3.0.32, RBS20 before 2.3.0.28, RBS40 before 2.3.0.28, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.78, WNDR3400v3 before 1.0.1.24, WNR2000v5 before 1.0.0.70, WNR2020 before 1.1.0.62, WNR3500Lv2 before 1.2.0.62, XR450 before 2.3.2.56, and XR500 before 2.3.2.56.	2021-12-26	not yet calculated	CVE-2021-45640 MISC
netgear -- d3600_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, D6200 before 1.1.00.34, D6220 before 1.0.0.52, D6400 before 1.0.0.86, D7000 before 1.0.1.74, D7000v2 before 1.0.0.53, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DC112A before 1.0.0.42, DGN2200Bv4 before 1.0.0.109, DGN2200v4 before 1.0.0.110, DM200 before 1.0.0.61, EX3700 before 1.0.0.76, EX3800 before 1.0.0.76, EX6120 before 1.0.0.46, EX6130 before 1.0.0.28, EX7000 before 1.0.1.78, PR2000 before 1.0.0.28, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6250 before 1.0.4.34, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 before 1.0.2.66, R6700v3 before 1.0.2.66, R6700 before 1.0.2.6, R6900 before 1.0.2.6, R7000 before 1.0.9.34, R7100LG before 1.0.0.50, R7500v2 before 1.0.3.40, R7900P before 1.4.1.50, R8000P before 1.4.1.50, R8900 before 1.0.4.12, R9000 before 1.0.4.12, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBR40 before 2.3.0.28, RBS40 before 2.3.0.28, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, WN3000RPv2 before 1.0.0.78, WNDR3400v3 before 1.0.1.24, WNR2000v5 before 1.0.0.70, WNR2020 before 1.1.0.62, and XR500 before 2.3.2.56.	2021-12-26	not yet calculated	CVE-2021-45641 MISC
netgear -- d6200_firmware	Certain NETGEAR devices are affected by Stored XSS. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6120 before 1.0.0.76, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R6850 before 1.1.0.78, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, and RAX40 before 1.0.3.62.	2021-12-26	not yet calculated	CVE-2021-45672 MISC
netgear -- d6200_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.42, R6080 before 1.0.0.42, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.64, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, AC2600 before 1.2.0.62, and WNR2020 before 1.1.0.62.	2021-12-26	not yet calculated	CVE-2021-45551 MISC
netgear -- d6200_firmware	Certain NETGEAR devices are affected by server-side injection. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	2021-12-26	not yet calculated	CVE-2021-45656 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- d6200_firmware	Certain NETGEAR devices are affected by server-side injection. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6050 before 1.0.1.26, JR6150 before 1.0.1.26, R6120 before 1.0.0.66, R6220 before 1.1.0.100, R6230 before 1.1.0.100, R6260 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, RBS50Y before 2.6.1.40, and WNR2020 before 1.1.0.62.	2021-12-26	not yet calculated	CVE-2021-45657 MISC
netgear -- d6220_firmware	NETGEAR D6220 devices before 1.0.0.76 are affected by command injection by an authenticated user.	2021-12-26	not yet calculated	CVE-2021-45531 MISC
netgear -- d6220_firmware	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.66, D6400 before 1.0.0.100, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, DC112A before 1.0.0.52, DGN2200v4 before 1.0.0.118, EAX80 before 1.0.1.64, R6250 before 1.0.4.48, R7000 before 1.0.11.110, R7100LG before 1.0.0.72, R7900 before 1.0.4.30, R7960P before 1.4.1.64, R8000 before 1.0.4.62, RAX200 before 1.0.3.106, RS400 before 1.5.1.80, XR300 before 1.0.3.68, R6400v2 before 1.0.4.106, R7000P before 1.3.2.132, R8000P before 1.4.1.64, RAX20 before 1.0.2.82, RAX45 before 1.0.2.82, RAX80 before 1.0.3.106, R6700v3 before 1.0.4.106, R6900P before 1.3.2.132, R7900P before 1.4.1.64, RAX15 before 1.0.2.82, RAX50 before 1.0.2.82, and RAX75 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45610 MISC
netgear -- d6220_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6220 before 1.0.0.68, D6400 before 1.0.0.102, D7000v2 before 1.0.0.74, D8500 before 1.0.3.60, DC112A before 1.0.0.56, R6300v2 before 1.0.4.50, R6400 before 1.0.1.68, R7000 before 1.0.11.116, R7100LG before 1.0.0.70, RBS40V before 2.6.2.8, RBW30 before 2.6.2.2, RS400 before 1.5.1.80, R7000P before 1.3.2.132, and R6900P before 1.3.2.132.	2021-12-26	not yet calculated	CVE-2021-45638 MISC
netgear -- d6220_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.68, D6400 before 1.0.0.102, D7000v2 before 1.0.0.66, D8500 before 1.0.3.58, DC112A before 1.0.0.54, EX7000 before 1.0.1.94, EX7500 before 1.0.0.72, R6250 before 1.0.4.48, R6300v2 before 1.0.4.52, R6400 before 1.0.1.70, R6400v2 before 1.0.4.102, R6700v3 before 1.0.4.102, R7000 before 1.0.11.116, R7100LG before 1.0.0.64, R7850 before 1.0.5.68, R7900 before 1.0.4.30, R7960P before 1.4.1.68, R8000 before 1.0.4.52, RAX200 before 1.0.2.88, RBS40V before 2.6.2.4, RS400 before 1.5.1.80, XR300 before 1.0.3.56, R7000P before 1.3.2.124, R8000P before 1.4.1.68, R8500 before 1.0.2.144, RAX80 before 1.0.3.102, R6900P before 1.3.2.124, R7900P before 1.4.1.68, R8300 before 1.0.2.144, RAX75 before 1.0.3.102, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45527 MISC
netgear -- d7000_firmware	NETGEAR D7000 devices before 1.0.1.82 are affected by authentication bypass.	2021-12-26	not yet calculated	CVE-2021-45497 MISC
netgear -- d7000_firmware	NETGEAR D7000 devices before 1.0.1.68 are affected by authentication bypass.	2021-12-26	not yet calculated	CVE-2021-45495 MISC
netgear -- d7000_firmware	NETGEAR D7000 devices before 1.0.1.82 are affected by authentication bypass.	2021-12-26	not yet calculated	CVE-2021-45496 MISC
netgear -- d7000_firmware	NETGEAR D7000 devices before 1.0.1.82 are affected by a stack-based buffer overflow by an unauthenticated attacker.	2021-12-26	not yet calculated	CVE-2021-45636 MISC
netgear -- d7000v2_firmware	Certain NETGEAR devices are affected by weak cryptography. This affects D7000v2 before 1.0.0.62, D8500 before 1.0.3.50, EX3700 before 1.0.0.84, EX3800 before 1.0.0.84, EX6120 before 1.0.0.54, EX6130 before 1.0.0.36, EX7000 before 1.0.1.90, R6250 before 1.0.4.42, R6400v2 before 1.0.4.98, R6700v3 before 1.0.4.98, R6900P before 1.3.2.124, R7000 before 1.0.11.106, R7000P before 1.3.2.124, R7100LG before 1.0.0.56, R7900 before 1.0.4.26, R8000 before 1.0.4.58, R8300 before 1.0.2.134, R8500 before 1.0.2.134, RS400 before 1.5.0.48, WNR3500Lv2 before 1.2.0.62, and XR300 before 1.0.3.50.	2021-12-26	not yet calculated	CVE-2021-45512 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- d7000v2_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7000v2 before 1.0.0.74, LAX20 before 1.1.6.28, MK62 before 1.0.6.116, MR60 before 1.0.6.116, MS60 before 1.0.6.116, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX43 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX35v2 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBR750 before 3.2.17.12, RBS750 before 3.2.17.12, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45614 MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by server-side injection. This affects D7800 before 1.0.1.58, DM200 before 1.0.0.66, EX2700 before 1.0.1.56, EX6150v2 before 1.0.1.86, EX6100v2 before 1.0.1.86, EX6200v2 before 1.0.1.78, EX6250 before 1.0.0.110, EX6410 before 1.0.0.110, EX6420 before 1.0.0.110, EX6400v2 before 1.0.0.110, EX7300 before 1.0.2.144, EX6400 before 1.0.2.144, EX7320 before 1.0.0.110, EX7300v2 before 1.0.0.110, R7500v2 before 1.0.3.48, R7800 before 1.0.2.68, R8900 before 1.0.5.2, R9000 before 1.0.5.2, RAX120 before 1.0.1.90, RBK40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, RBS50Y before 2.6.1.40, WN3000RPv2 before 1.0.0.78, WN3000RPv3 before 1.0.2.80, WNR2000v5 before 1.0.0.72, XR500 before 2.3.2.56, and XR700 before 1.0.1.20.	2021-12-26	not yet calculated	CVE-2021-45658 MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.66, EX2700 before 1.0.1.68, WN3000RPv2 before 1.0.0.90, WN3000RPv3 before 1.0.2.100, LBR1020 before 2.6.5.20, LBR20 before 2.6.5.32, R6700AX before 1.0.10.110, R7800 before 1.0.2.86, R8900 before 1.0.5.38, R9000 before 1.0.5.38, RAX10 before 1.0.10.110, RAX120v1 before 1.2.3.28, RAX120v2 before 1.2.3.28, RAX70 before 1.0.10.110, RAX78 before 1.0.10.110, XR450 before 2.3.2.130, XR500 before 2.3.2.130, and XR700 before 1.0.1.46.	2021-12-26	not yet calculated	CVE-2021-45602 MISC MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. A UPnP request reveals a device's serial number, which can be used for a password reset. This affects D7800 before 1.0.1.66, EX2700 before 1.0.1.68, WN3000RPv2 before 1.0.0.90, WN3000RPv3 before 1.0.2.100, LBR1020 before 2.6.5.20, LBR20 before 2.6.5.32, R6700AX before 1.0.10.110, R7800 before 1.0.2.86, R8900 before 1.0.5.38, R9000 before 1.0.5.38, RAX10 before 1.0.10.110, RAX120v1 before 1.2.3.28, RAX120v2 before 1.2.3.28, RAX70 before 1.0.10.110, RAX78 before 1.0.10.110, XR450 before 2.3.2.130, XR500 before 2.3.2.130, and XR700 before 1.0.1.46.	2021-12-26	not yet calculated	CVE-2021-45603 MISC MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.64, EX6250 before 1.0.0.134, EX7700 before 1.0.0.222, LBR20 before 2.6.3.50, RBS50Y before 2.7.3.22, R8900 before 1.0.5.26, R9000 before 1.0.5.26, XR450 before 2.3.2.66, XR500 before 2.3.2.66, XR700 before 1.0.1.36, EX7320 before 1.0.0.134, RAX120 before 1.2.2.24, EX7300v2 before 1.0.0.134, RAX120v2 before 1.2.2.24, EX6410 before 1.0.0.134, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, EX6420 before 1.0.0.134, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, EX6400v2 before 1.0.0.134, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45642 MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.58, R7500v2 before 1.0.3.48, R7800 before 1.0.2.68, R8900 before 1.0.5.2, R9000 before 1.0.5.2, RAX120 before 1.0.1.108, and XR700 before 1.0.1.20.	2021-12-26	not yet calculated	CVE-2021-45552 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- d7800_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.60, DM200 before 1.0.0.66, EX2700 before 1.0.1.56, EX6150v2 before 1.0.1.86, EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.128, EX6400 before 1.0.2.144, EX6400v2 before 1.0.0.128, EX6410 before 1.0.0.128, EX6420 before 1.0.0.128, EX7300 before 1.0.2.144, EX7300v2 before 1.0.0.128, EX7320 before 1.0.0.128, R7500v2 before 1.0.3.46, R7800 before 1.0.2.74, R8900 before 1.0.5.26, R9000 before 1.0.5.2, RAX120 before 1.0.1.128, WN3000RPv2 before 1.0.0.78, WN3000RPv3 before 1.0.2.80, WNR2000v5 before 1.0.0.74, XR500 before 2.3.2.66, RBK20 before 2.7.3.22, RBR20 before 2.7.3.22, RBS20 before 2.7.3.22, RBK40 before 2.7.3.22, RBR40 before 2.7.3.22, and RBS40 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45548 MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7800 before 1.0.1.64, EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.134, EX7700 before 1.0.0.216, EX8000 before 1.0.1.232, LBR20 before 2.6.3.50, R7800 before 1.0.2.80, R8900 before 1.0.5.26, R9000 before 1.0.5.26, RAX120 before 1.2.0.16, RBS50Y before 1.0.0.56, WNR2000v5 before 1.0.0.76, XR450 before 2.3.2.114, XR500 before 2.3.2.114, XR700 before 1.0.1.36, EX6150v2 before 1.0.1.98, EX7300 before 1.0.2.158, EX7320 before 1.0.0.134, EX6100v2 before 1.0.1.98, EX6400 before 1.0.2.158, EX7300v2 before 1.0.0.134, EX6410 before 1.0.0.134, RBR10 before 2.6.1.44, RBR20 before 2.6.2.104, RBR40 before 2.6.2.104, RBR50 before 2.7.2.102, EX6420 before 1.0.0.134, RBS10 before 2.6.1.44, RBS20 before 2.6.2.104, RBS40 before 2.6.2.104, RBS50 before 2.7.2.102, EX6400v2 before 1.0.0.134, RBK12 before 2.6.1.44, RBK20 before 2.6.2.104, RBK40 before 2.6.2.104, and RBK50 before 2.7.2.102.	2021-12-26	not yet calculated	CVE-2021-45618 MISC
netgear -- d7800_firmware	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.68, R6400v2 before 1.0.4.122, and R6700v3 before 1.0.4.122.	2021-12-26	not yet calculated	CVE-2021-45608 MISC
netgear -- d8500_firmware	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.58, R6250 before 1.0.4.48, R7000 before 1.0.11.116, R7100LG before 1.0.0.64, R7900 before 1.0.4.38, R8300 before 1.0.2.144, R8500 before 1.0.2.144, XR300 before 1.0.3.68, R7000P before 1.3.2.132, and R6900P before 1.3.2.132.	2021-12-26	not yet calculated	CVE-2021-45609 MISC
netgear -- dc112a_firmware	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects DC112A before 1.0.0.52, R6400 before 1.0.1.68, RAX200 before 1.0.3.106, WNDR3400v3 before 1.0.1.38, XR300 before 1.0.3.68, R8500 before 1.0.2.144, RAX75 before 1.0.3.106, R8300 before 1.0.2.144, and RAX80 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45611 MISC
netgear -- eax20_firmware	Certain NETGEAR devices are affected by stored XSS. This affects EAX20 before 1.0.0.36, EAX80 before 1.0.1.62, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, RBW30 before 2.6.1.4, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, and RBS40V before 2.6.1.4.	2021-12-26	not yet calculated	CVE-2021-45665 MISC
netgear -- eax20_firmware	Certain NETGEAR devices are affected by stored XSS. This affects EAX20 before 1.0.0.48, EAX80 before 1.0.1.64, EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, EX6130 before 1.0.0.44, EX7500 before 1.0.0.72, R7960P before 1.4.1.66, R7900P before 1.4.1.66, R8000P before 1.4.1.66, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.72, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45668 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- eax80_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects EAX80 before 1.0.1.62, EX7000 before 1.0.1.104, R6120 before 1.0.0.76, R6220 before 1.1.0.110, R6230 before 1.1.0.110, R6260 before 1.1.0.78, R6850 before 1.1.0.78, R6350 before 1.1.0.78, R6330 before 1.1.0.78, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6700v2 before 1.2.0.76, R7000 before 1.0.11.116, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, R7900 before 1.0.4.38, R7960P before 1.4.1.66, R8000 before 1.0.4.68, R7900P before 1.4.1.66, R8000P before 1.4.1.66, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.72, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45647 MISC
netgear -- ex6000_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects EX6000 before 1.0.0.38, EX6120 before 1.0.0.48, EX6130 before 1.0.0.30, R6300v2 before 1.0.4.52, R6400 before 1.0.1.52, R7000 before 1.0.11.126, R7900 before 1.0.4.30, R8000 before 1.0.4.52, R7000P before 1.3.2.124, R8000P before 1.4.1.50, RAX80 before 1.0.3.88, R6900P before 1.3.2.124, R7900P before 1.4.1.50, and RAX75 before 1.0.3.88.	2021-12-26	not yet calculated	CVE-2021-45526 MISC
netgear -- ex6100v2_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects EX6100v2 before 1.0.1.106, EX6150v2 before 1.0.1.106, EX6250 before 1.0.0.146, EX6400 before 1.0.2.164, EX6400v2 before 1.0.0.146, EX6410 before 1.0.0.146, EX6420 before 1.0.0.146, EX7300 before 1.0.2.164, EX7300v2 before 1.0.0.146, EX7320 before 1.0.0.146, EX7700 before 1.0.0.222, LBR1020 before 2.6.5.16, LBR20 before 2.6.5.2, RBK352 before 4.3.4.7, RBK50 before 2.7.3.22, RBR350 before 4.3.4.7, RBR50 before 2.7.3.22, and RBS350 before 4.3.4.7.	2021-12-26	not yet calculated	CVE-2021-45648 MISC
netgear -- ex6120_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects EX6120 before 1.0.0.66, EX6130 before 1.0.0.46, EX7000 before 1.0.1.106, EX7500 before 1.0.1.76, EX3700 before 1.0.0.94, EX3800 before 1.0.0.94, RBR850 before 4.6.3.9, RBS850 before 4.6.3.9, and RBK852 before 4.6.3.9.	2021-12-26	not yet calculated	CVE-2021-45533 MISC
netgear -- ex6200v2_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects EX6200v2 before 1.0.1.86, EX6250 before 1.0.0.134, EX7700 before 1.0.0.216, EX8000 before 1.0.1.232, LBR1020 before 2.6.3.58, LBR20 before 2.6.3.50, R7800 before 1.0.2.80, R8900 before 1.0.5.26, R9000 before 1.0.5.26, RBS50Y before 2.7.3.22, WNR2000v5 before 1.0.0.76, XR700 before 1.0.1.36, EX6150v2 before 1.0.1.98, EX7300 before 1.0.2.158, EX7320 before 1.0.0.134, RAX10 before 1.0.2.88, RAX120 before 1.2.0.16, RAX70 before 1.0.2.88, EX6100v2 before 1.0.1.98, EX6400 before 1.0.2.158, EX7300v2 before 1.0.0.134, R6700AX before 1.0.2.88, RAX120v2 before 1.2.0.16, RAX78 before 1.0.2.88, EX6410 before 1.0.0.134, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR350 before 4.3.4.7, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, EX6420 before 1.0.0.134, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS350 before 4.3.4.7, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, EX6400v2 before 1.0.0.134, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK352 before 4.3.4.7, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45619 MISC
netgear -- ex7000_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects EX7000 before 1.0.1.80, R6400 before 1.0.1.50, R6400v2 before 1.0.4.118, R6700 before 1.0.2.8, R6700v3 before 1.0.4.118, R6900 before 1.0.2.8, R6900P before 1.3.2.124, R7000 before 1.0.9.88, R7000P before 1.3.2.124, R7900 before 1.0.3.18, R7900P before 1.4.1.50, R8000 before 1.0.4.46, R8000P before 1.4.1.50, RAX80 before 1.0.1.56, and WNR3500Lv2 before 1.2.0.62.	2021-12-26	not yet calculated	CVE-2021-45525 MISC
netgear -- ex7500_firmware	Certain NETGEAR devices are affected by denial of service. This affects EX7500 before 1.0.0.72, RBS40V before 2.6.1.4, RBW30 before 2.6.1.4, RBRE960 before 6.0.3.68, RBSE960 before 6.0.3.68, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, and RBK852 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45515 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- gc108p_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects GC108P before 1.0.8.2, GC108PP before 1.0.8.2, GS108Tv3 before 7.0.7.2, GS110TPv3 before 7.0.7.2, GS110TPP before 7.0.7.2, GS110TUP before 1.0.5.3, GS710TUP before 1.0.5.3, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS710TUP before 1.0.5.3, GS716TP before 1.0.4.2, GS716TPP before 1.0.4.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS724TPP before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS752TPv2 before 6.0.8.2, GS752TPP before 6.0.8.2, GS750E before 1.0.1.10, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	2021-12-26	not yet calculated	CVE-2021-45557 MISC
netgear -- genie_installer	All known versions of the Netgear Genie Installer for macOS contain a local privilege escalation vulnerability. The installer of the macOS version of Netgear Genie handles certain files in an insecure way. A malicious actor who has local access to the endpoint on which the software is going to be installed may overwrite certain files to obtain privilege escalation to root.	2021-12-30	not yet calculated	CVE-2021-20172 MISC
netgear -- gs108tv2_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects GS108Tv2 before 5.4.2.36, GS110TPP before 7.0.7.2, GS110TPv2 before 5.4.2.36., GS110TPv3 before 7.0.7.2, GS308T before 1.0.3.2, GS310TP before 1.0.3.2, GS724TPP before 2.0.6.3, GS724TPv2 before 2.0.6.3, GS728TPPv2 before 6.0.8.2, GS728TPv2 before 6.0.8.2, GS752TPP before 6.0.8.2, GS752TPv2 before 6.0.8.2, MS510TXM before 1.0.4.2, and MS510TXUP before 1.0.4.2.	2021-12-26	not yet calculated	CVE-2021-45556 MISC
netgear -- gs108tv2_firmware	Certain NETGEAR devices are affected by stored XSS. This affects GS108Tv2 before 5.4.2.36 and GS110TPv2 before 5.4.2.36.	2021-12-26	not yet calculated	CVE-2021-45677 MISC
netgear -- lax20_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects LAX20 before 1.1.6.28, MK62 before 1.1.6.122, MR60 before 1.1.6.122, MS60 before 1.1.6.122, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.116, R7000P before 1.3.3.140, R7850 before 1.0.5.68, R7900 before 1.0.4.38, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX15 before 1.0.3.96, RAX20 before 1.0.3.96, RAX200 before 1.0.4.120, RAX35v2 before 1.0.3.96, RAX40v2 before 1.0.3.96, RAX43 before 1.0.3.96, RAX45 before 1.0.3.96, RAX50 before 1.0.3.96, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RS400 before 1.5.1.80, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45549 MISC
netgear -- lbr20_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects LBR20 before 2.6.3.50, RBS50Y before 2.7.3.22, RBR10 before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, RBS10 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, RBK12 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45595 MISC
netgear -- mediatek	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-32469 MISC
netgear -- mediatek	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-32468 MISC
netgear -- mediatek	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-32467 MISC
netgear -- mediatek_microchips	MediaTek microchips, as used in NETGEAR devices through 2021-12-13 and other devices, mishandle attempts at Wi-Fi authentication flooding.	2021-12-26	not yet calculated	CVE-2021-41788 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37571 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37570 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-37584 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37566 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-37563 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-37562 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37565 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37572 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-37561 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-35055 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37569 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37583 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37568 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37564 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle the WPS (Wi-Fi Protected Setup) protocol.	2021-12-26	not yet calculated	CVE-2021-37560 MISC
netgear -- multiple_devices	MediaTek microchips, as used in NETGEAR devices through 2021-11-11 and other devices, mishandle IEEE 1905 protocols.	2021-12-26	not yet calculated	CVE-2021-37567 MISC
netgear -- nighthawk	Netgear Nighthawk R6700 version 1.0.4.120 makes use of a hardcoded credential. It does not appear that normal users are intended to be able to manipulate configuration backups due to the fact that they are encrypted/obfuscated. By extracting the configuration using readily available public tools, a user can reconfigure settings not intended to be manipulated, repackage the configuration, and restore a backup causing these settings to be changed.	2021-12-30	not yet calculated	CVE-2021-45732 MISC
netgear -- nighthawk_r6700	Netgear Nighthawk R6700 version 1.0.4.120 does not utilize secure communication methods to the web interface. By default, all communication to/from the device's web interface is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext.	2021-12-30	not yet calculated	CVE-2021-20174 MISC
netgear -- nighthawk_r6700	Netgear Nighthawk R6700 version 1.0.4.120 does not utilize secure communication methods to the SOAP interface. By default, all communication to/from the device's SOAP Interface (port 5000) is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext	2021-12-30	not yet calculated	CVE-2021-20175 MISC
netgear -- nighthawk_r6700	Netgear Nighthawk R6700 version 1.0.4.120 does not have sufficient protections for the UART console. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection and execute commands as the root user without authentication.	2021-12-30	not yet calculated	CVE-2021-23147 MISC
netgear -- nighthawk_r6700	Netgear Nighthawk R6700 version 1.0.4.120 stores sensitive information in plaintext. All usernames and passwords for the device's associated services are stored in plaintext on the device. For example, the admin password is stored in plaintext in the primary configuration file on the device.	2021-12-30	not yet calculated	CVE-2021-45077 MISC
netgear -- nighthawk_r6700	Netgear Nighthawk R6700 version 1.0.4.120 contains a command injection vulnerability in update functionality of the device. By triggering a system update check via the SOAP interface, the device is susceptible to command injection via preconfigured values.	2021-12-30	not yet calculated	CVE-2021-20173 MISC
netgear -- r6120_firmware	Certain NETGEAR devices are affected by stored XSS. This affects R6120 before 1.0.0.76, R6260 before 1.1.0.78, R6850 before 1.1.0.78, R6350 before 1.1.0.78, R6330 before 1.1.0.78, R6800 before 1.2.0.76, R6700v2 before 1.2.0.76, R6900v2 before 1.2.0.76, R7200 before 1.2.0.76, R7350 before 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, and AC2600 before 1.2.0.76.	2021-12-26	not yet calculated	CVE-2021-45675 MISC
netgear -- r6260_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6260 before 1.1.0.76, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, and AC2600 before 1.2.0.62.	2021-12-26	not yet calculated	CVE-2021-45573 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- r6260_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6260 before 1.1.0.76, R6800 before 1.2.0.62, R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, R7450 before 1.2.0.62, AC2100 before 1.2.0.62, AC2400 before 1.2.0.62, and AC2600 before 1.2.0.62.	2021-12-26	not yet calculated	CVE-2021-45637 MISC
netgear -- r6300v2_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R6300v2 before 1.0.4.52, R6400 before 1.0.1.52, R6900 before 1.0.2.8, R7000 before 1.0.9.88, R7900 before 1.0.3.18, R8000 before 1.0.4.46, R7900P before 1.4.1.50, R8000P before 1.4.1.50, RAX75 before 1.0.3.88, RAX80 before 1.0.3.88, and WNR3500Lv2 before 1.2.0.62.	2021-12-26	not yet calculated	CVE-2021-45528 MISC
netgear -- r6400_firmware	Certain NETGEAR devices are affected by denial of service. This affects R6400 before 1.0.1.70, R7000 before 1.0.11.126, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R8000 before 1.0.4.74, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.	2021-12-26	not yet calculated	CVE-2021-45516 MISC
netgear -- r6400_firmware	NETGEAR R6400 devices before 1.0.1.70 are affected by server-side injection.	2021-12-26	not yet calculated	CVE-2021-45655 MISC
netgear -- r6400_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400 before 1.0.1.70, R7000 before 1.0.11.126, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RS400 before 1.5.1.80, R6400v2 before 1.0.4.118, R7000P before 1.3.3.140, RAX80 before 1.0.4.120, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, and RAX75 before 1.0.4.120.	2021-12-26	not yet calculated	CVE-2021-45606 MISC
netgear -- r6400_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400 before 1.0.1.74, R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R7000 before 1.0.11.126, R6900P before 1.3.3.140, R7000P before 1.3.3.140, and R8000 before 1.0.4.74.	2021-12-26	not yet calculated	CVE-2021-45554 MISC
netgear -- r6400_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400 before 1.0.1.68, R7000 before 1.0.11.116, R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7900 before 1.0.4.38, RAX75 before 1.0.3.102, RAX80 before 1.0.3.102, and XR300 before 1.0.3.50.	2021-12-26	not yet calculated	CVE-2021-45605 MISC
netgear -- r6400v2_firmware	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, RAX200 before 1.0.5.126, RAX75 before 1.0.5.126, and RAX80 before 1.0.5.126.	2021-12-26	not yet calculated	CVE-2021-45607 MISC
netgear -- r6400v2_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6400v2 before 1.0.4.118, R6700v3 before 1.0.4.118, and XR1000 before 1.0.0.58.	2021-12-26	not yet calculated	CVE-2021-45643 MISC
netgear -- r6400v2_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6400v2 before 1.0.4.84, R6700v3 before 1.0.4.84, R7000 before 1.0.11.126, R6900P before 1.3.2.126, and R7000P before 1.3.2.126.	2021-12-26	not yet calculated	CVE-2021-45649 MISC
netgear -- r6700v2_firmware	NETGEAR R6700v2 devices before 1.2.0.88 are affected by authentication bypass.	2021-12-26	not yet calculated	CVE-2021-45498 MISC
netgear -- r6900p_firmware	Certain NETGEAR devices are affected by privilege escalation. This affects R6900P before 1.3.3.140, R7000 before 1.0.11.126, R7000P before 1.3.3.140, and RS400 before 1.5.1.80.	2021-12-26	not yet calculated	CVE-2021-45679 MISC
netgear -- r6900p_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects R6900P before 1.3.3.140, R7000P before 1.3.3.140, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000P before 1.4.2.84, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45499 MISC
netgear -- r7000_firmware	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R7000 before 1.0.11.126, R7960P before 1.4.2.84, R8000 before 1.0.4.74, RAX200 before 1.0.4.120, R8000P before 1.4.2.84, RAX20 before 1.0.2.82, RAX45 before 1.0.2.82, RAX80 before 1.0.4.120, R7900P before 1.4.2.84, RAX15 before 1.0.2.82, RAX50 before 1.0.2.82, and RAX75 before 1.0.4.120.	2021-12-26	not yet calculated	CVE-2021-45530 MISC
netgear -- r7000_firmware	NETGEAR R7000 devices before 1.0.11.116 are affected by disclosure of sensitive information.	2021-12-26	not yet calculated	CVE-2021-45646 MISC
netgear -- r7000_firmware	NETGEAR R7000 devices before 1.0.9.88 are affected by stored XSS.	2021-12-26	not yet calculated	CVE-2021-45662 MISC
netgear -- r7000_firmware	NETGEAR R7000 devices before 1.0.9.42 are affected by a buffer overflow by an authenticated user.	2021-12-26	not yet calculated	CVE-2021-45523 MISC
netgear -- r7000_firmware	NETGEAR R7000 devices before 1.0.11.126 are affected by stored XSS.	2021-12-26	not yet calculated	CVE-2021-45664 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- r7000_firmware	NETGEAR R7000 devices before 1.0.11.126 are affected by stored XSS.	2021-12-26	not yet calculated	CVE-2021-45663 MISC
netgear -- r7000_firmware	Certain NETGEAR devices are affected by stored XSS. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX75 before 1.0.3.106, and RAX80 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45674 MISC
netgear -- r7000_firmware	Certain NETGEAR devices are affected by stored XSS. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RAX200 before 1.0.3.106, R7000P before 1.3.3.140, RAX80 before 1.0.3.106, R6900P before 1.3.3.140, and RAX75 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45673 MISC
netgear -- r7000_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7000 before 1.0.11.126, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX45 before 1.0.2.66, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX50 before 1.0.2.66, and RAX75 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45540 MISC
netgear -- r7000_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R7000 before 1.0.11.110, R7900 before 1.0.4.30, R8000 before 1.0.4.62, RS400 before 1.5.1.80, R6400v2 before 1.0.4.102, R7000P before 1.3.2.126, R6700v3 before 1.0.4.102, and R6900P before 1.3.2.126.	2021-12-26	not yet calculated	CVE-2021-45650 MISC
netgear -- r7000p_firmware	Certain NETGEAR devices are affected by authentication bypass. This affects R7000P before 1.3.3.140 and R8000 before 1.0.4.68.	2021-12-26	not yet calculated	CVE-2021-45500 MISC
netgear -- r7800_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects R7800 before 1.0.2.74, R9000 before 1.0.5.2, and XR500 before 2.3.2.66.	2021-12-26	not yet calculated	CVE-2021-45623 MISC
netgear -- r7850_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45544 MISC
netgear -- r7850_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45546 MISC
netgear -- r7850_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45545 MISC
netgear -- r7850_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7850 before 1.0.5.74, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK752 before 3.2.17.12, RBK852 before 3.2.17.12, RBR750 before 3.2.17.12, RBR850 before 3.2.17.12, RBS750 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45547 MISC
netgear -- r7900_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900 before 1.0.4.38, R7900P before 1.4.2.84, R8000 before 1.0.4.68, R8000P before 1.4.2.84, RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45541 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- r7900p_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.28, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.28, and RAX75 before 1.0.3.106.	2021-12-26	not yet calculated	CVE-2021-45539 MISC
netgear -- r7900p_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7900P before 1.4.2.84, R7960P before 1.4.2.84, and R8000P before 1.4.2.84.	2021-12-26	not yet calculated	CVE-2021-45555 MISC
netgear -- r8000_firmware	NETGEAR R8000 devices before 1.0.4.62 are affected by a buffer overflow by an authenticated user.	2021-12-26	not yet calculated	CVE-2021-45524 MISC
netgear -- r8000_firmware	NETGEAR R8000 devices before 1.0.4.76 are affected by command injection by an authenticated user.	2021-12-26	not yet calculated	CVE-2021-45532 MISC
netgear -- r8000_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R8000 before 1.0.4.74, RAX200 before 1.0.4.120, R8000P before 1.4.2.84, R7900P before 1.4.2.84, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, and RBK852 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45543 MISC
netgear -- rax200_firmware	NETGEAR RAX200 devices before 1.0.5.132 are affected by insecure code.	2021-12-26	not yet calculated	CVE-2021-45678 MISC
netgear -- rax200_firmware	Certain NETGEAR devices are affected by stored XSS. This affects RAX200 before 1.0.5.126, RAX20 before 1.0.2.82, RAX80 before 1.0.5.126, RAX15 before 1.0.2.82, and RAX75 before 1.0.5.126.	2021-12-26	not yet calculated	CVE-2021-45676 MISC
netgear -- rax200_firmware	Certain NETGEAR devices are affected by stored XSS. This affects RAX200 before 1.0.3.106, MR60 before 1.0.6.110, RAX20 before 1.0.2.82, RAX45 before 1.0.2.72, RAX80 before 1.0.3.106, MS60 before 1.0.6.110, RAX15 before 1.0.2.82, RAX50 before 1.0.2.72, RAX75 before 1.0.3.106, RBR750 before 3.2.16.6, RBR850 before 3.2.16.6, RBS750 before 3.2.16.6, RBS850 before 3.2.16.6, RBK752 before 3.2.16.6, and RBK852 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45669 MISC
netgear -- rax200_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user . This affects RAX200 before 1.0.3.106, RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45537 MISC
netgear -- rax200_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.	2021-12-26	not yet calculated	CVE-2021-45542 MISC
netgear -- rax200_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.3.106, RAX80 before 1.0.3.106, RAX75 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45535 MISC
netgear -- rax35_firmware	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RAX35 before 1.0.4.102, RAX38 before 1.0.4.102, and RAX40 before 1.0.4.102.	2021-12-26	not yet calculated	CVE-2021-45493 MISC
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 contains a command injection vulnerability. The readycloud cgi application is vulnerable to command injection in the name parameter.	2021-12-30	not yet calculated	CVE-2021-20167 MISC
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 does not have sufficient protections to the UART interface. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection, login with default credentials, and execute commands as the root user. These default credentials are admin:admin.	2021-12-30	not yet calculated	CVE-2021-20168 MISC
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 does not utilize secure communications to the web interface. By default, all communication to/from the device is sent via HTTP, which causes potentially sensitive information (such as usernames and passwords) to be transmitted in cleartext.	2021-12-30	not yet calculated	CVE-2021-20169 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 makes use of hardcoded credentials. It does not appear that normal users are intended to be able to manipulate configuration backups due to the fact that they are encrypted. This encryption is accomplished via a password-protected zip file with a hardcoded password (RAX50w!a4udk). By unzipping the configuration using this password, a user can reconfigure settings not intended to be manipulated, re-zip the configuration, and restore a backup causing these settings to be changed.	2021-12-30	not yet calculated	CVE-2021-20170 MISC
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 stores sensitive information in plaintext. All usernames and passwords for the device's associated services are stored in plaintext on the device. For example, the admin password is stored in plaintext in the primary configuration file on the device.	2021-12-30	not yet calculated	CVE-2021-20171 MISC
netgear -- rax43_firmware	Netgear RAX43 version 1.0.3.96 contains a buffer overrun vulnerability. The URL parsing functionality in the cgi-bin endpoint of the router containers a buffer overrun issue that can redirection control flow of the applicaiton.	2021-12-30	not yet calculated	CVE-2021-20166 MISC
netgear -- rax75_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45538 MISC
netgear -- rax75_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX75 before 1.0.3.106, RAX80 before 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45536 MISC
netgear -- rbk20_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK20 before 2.6.1.36, RBR20 before 2.6.1.36, RBS20 before 2.6.1.38, RBK40 before 2.6.1.36, RBR40 before 2.6.1.36, RBS40 before 2.6.1.38, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, and RBS50Y before 2.6.1.40.	2021-12-26	not yet calculated	CVE-2021-45626 MISC
netgear -- rbk352_firmware	Certain NETGEAR devices are affected by a hardcoded password. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	2021-12-26	not yet calculated	CVE-2021-45521 MISC
netgear -- rbk352_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	2021-12-26	not yet calculated	CVE-2021-45653 MISC
netgear -- rbk352_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	2021-12-26	not yet calculated	CVE-2021-45652 MISC
netgear -- rbk352_firmware	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	2021-12-26	not yet calculated	CVE-2021-45494 MISC
netgear -- rbk352_firmware	Certain NETGEAR devices are affected by a hardcoded password. This affects RBK352 before 4.4.0.10, RBR350 before 4.4.0.10, and RBS350 before 4.4.0.10.	2021-12-26	not yet calculated	CVE-2021-45520 MISC
netgear -- rbk40_firmware	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	2021-12-26	not yet calculated	CVE-2021-45660 MISC
netgear -- rbk40_firmware	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	2021-12-26	not yet calculated	CVE-2021-45659 MISC
netgear -- rbk40_firmware	Certain NETGEAR devices are affected by server-side injection. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	2021-12-26	not yet calculated	CVE-2021-45661 MISC
netgear -- rbk50_firmware	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects RBK50 before 2.7.3.22, RBR50 before 2.7.3.22, and RBS50 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45651 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45569 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45588 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45574 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45570 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R7000 before 1.0.11.126, R6900P before 1.3.2.126, and R7000P before 1.3.2.126.	2021-12-26	not yet calculated	CVE-2021-45553 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45562 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45561 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45559 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45571 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45568 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45590 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45589 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45591 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45587 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45576 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45585 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45583 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45582 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45575 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45581 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45580 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45586 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45579 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45578 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45577 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45566 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45560 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45565 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45564 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45563 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45572 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45592 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45567 MISC
netgear -- rbk752_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, and RBS850 before 3.2.16.6.	2021-12-26	not yet calculated	CVE-2021-45558 MISC
netgear -- rbr20_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.2.102, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBR50 before 2.7.2.102, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.2.102.	2021-12-26	not yet calculated	CVE-2021-45593 MISC
netgear -- rbs50y_firmware	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBS50Y before 2.7.3.22, RBR20 before 2.7.3.22, RBR40 before 2.7.3.22, RBR50 before 2.7.3.22, RBS20 before 2.7.3.22, RBS40 before 2.7.3.22, RBS50 before 2.7.3.22, RBK20 before 2.7.3.22, RBK40 before 2.7.3.22, and RBK50 before 2.7.3.22.	2021-12-26	not yet calculated	CVE-2021-45594 MISC
netgear -- rbs50y_firmware	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects RBS50Y before 2.7.0.122, SRK60 before 2.7.0.122, SRR60 before 2.7.0.122, SRS60 before 2.7.0.122, SXK30 before 3.2.33.108, SXR30 before 3.2.33.108, SXS30 before 3.2.33.108, and SRC60 before 2.7.0.122.	2021-12-26	not yet calculated	CVE-2021-45645 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	2021-12-26	not yet calculated	CVE-2021-45519 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by command injection by an unauthenticated attacker.	2021-12-26	not yet calculated	CVE-2021-45513 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by disclosure of sensitive information.	2021-12-26	not yet calculated	CVE-2021-45654 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	2021-12-26	not yet calculated	CVE-2021-45518 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by authentication bypass.	2021-12-26	not yet calculated	CVE-2021-45510 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by denial of service.	2021-12-26	not yet calculated	CVE-2021-45517 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by command injection by an unauthenticated attacker.	2021-12-26	not yet calculated	CVE-2021-45514 MISC
netgear -- xr1000_firmware	NETGEAR XR1000 devices before 1.0.0.58 are affected by a hardcoded password.	2021-12-26	not yet calculated	CVE-2021-45522 MISC
netgear -- xr300_firmware	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects XR300 before 1.0.3.68, R7000P before 1.3.3.140, and R6900P before 1.3.3.140.	2021-12-26	not yet calculated	CVE-2021-45625 MISC
netgen -- tags_bundle	Netgen Tags Bundle 3.4.x before 3.4.11 and 4.0.x before 4.0.15 allows XSS in the Tags Admin interface.	2021-12-27	not yet calculated	CVE-2021-45895 MISC MISC
nettmp -- nettmp	Nettmp NNT 5.1 is affected by a SQL injection vulnerability. An attacker can bypass authentication and access the panel with an administrative account.	2021-12-28	not yet calculated	CVE-2021-45814 MISC MISC
nokia -- fastmile	Nokia FastMile 3TG00118ABAD52 devices allow privilege escalation by an authenticated user via is_ctc_admin=1 to login_web_app.cgi and use of Import Config File.	2021-12-27	not yet calculated	CVE-2021-45896 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nuuo -- network_video_recorder	NUUO Network Video Recorder NVRsolo 3.9.1 is affected by a Cross Site Scripting (XSS) vulnerability. An attacker can steal the user's session by injecting malicious JavaScript codes which leads to session hijacking.	2021-12-28	not yet calculated	CVE-2021-45812 MISC
open_asset -- import_library	Open Asset Import Library (aka assimp) 5.1.0 and 5.1.1 has a heap-based buffer overflow in _m3d_safestr (called from m3d_load and Assimp::M3DWrapper::M3DWrapper).	2022-01-01	not yet calculated	CVE-2021-45948 MISC MISC
openexr -- openexr	OpenEXR 3.1.0 through 3.1.3 has a heap-based buffer overflow in Imf_3_1::LineCompositeTask::execute (called from IlmThread_3_1::NullThreadPoolProvider::addTask and IlmThread_3_1::ThreadPool::addGlobalTask).	2022-01-01	not yet calculated	CVE-2021-45942 MISC MISC MISC
openwrt -- openwrt	OpenWrt 21.02.1 allows XSS via the Traffic Rules Name screen.	2021-12-27	not yet calculated	CVE-2021-45905 MISC
openwrt -- openwrt	OpenWrt 21.02.1 allows XSS via the Port Forwards Add Name screen.	2021-12-27	not yet calculated	CVE-2021-45904 MISC
openwrt -- openwrt	OpenWrt 21.02.1 allows XSS via the NAT Rules Name screen.	2021-12-27	not yet calculated	CVE-2021-45906 MISC
oppo -- oppo	ColorOS pregrant dangerous permissions to apps which are listed in a whitelist xml named default-grant-permissions.But some apps in whitelist is not installed, attacker can disguise app with the same package name to obtain dangerous permission.	2021-12-27	not yet calculated	CVE-2021-23244 MISC
parse-link-header -- parse-link-header	The package parse-link-header before 2.0.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the checkHeader function.	2021-12-24	not yet calculated	CVE-2021-23490 CONFIRM CONFIRM CONFIRM
philips -- patient_information_center_ix	Patient Information Center iX (PIC iX) Versions C.02 and C.03 receives input or data, but does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly.	2021-12-27	not yet calculated	CVE-2021-43548 MISC
philips -- patient_information_center_ix	The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information, which affects the communications between Patient Information Center iX (PIC iX) Versions C.02 and C.03 and Efficia CM Series Revisions A.01 to C.0x and 4.0.	2021-12-27	not yet calculated	CVE-2021-43550 MISC
philips -- patient_information_center_ix	The use of a hard-coded cryptographic key significantly increases the possibility encrypted data may be recovered from the Patient Information Center iX (PIC iX) Versions B.02, C.02, and C.03.	2021-12-27	not yet calculated	CVE-2021-43552 MISC
pjsip -- pjsip	PJSIP is a free and open source multimedia communication library. In version 2.11.1 and prior, if incoming RTCP XR message contain block, the data field is not checked against the received packet size, potentially resulting in an out-of-bound read access. This affects all users that use PJMEDIA and RTCP XR. A malicious actor can send a RTCP XR message with an invalid packet size.	2021-12-27	not yet calculated	CVE-2021-43845 MISC CONFIRM MISC
poly -- poly_trio_8800	A remote code execution issue in the ping command on Poly Trio 8800 5.7.1.4145 devices allows remote authenticated users to execute commands via unspecified vectors.	2021-12-28	not yet calculated	CVE-2018-17875 MISC MISC
qibosoft -- qibosoft	A Cross-Site Request Forgery (CSRF) in /admin/index.php?lfj=member&action=editmember of Qibosoft v7 allows attackers to arbitrarily add administrator accounts.	2021-12-27	not yet calculated	CVE-2020-20945 MISC MISC
qibosoft -- qibosoft	A Cross-Site Request Forgery (CSRF) in /member/post.php?job=postnew&step=post of Qibosoft v7 allows attackers to force victim users into arbitrarily publishing new articles via a crafted URL.	2021-12-27	not yet calculated	CVE-2020-20943 MISC
qibosoft -- qibosoft	Qibosoft v7 contains a stored cross-site scripting (XSS) vulnerability in the component /admin/index.php?lfj=friendlink&action=add.	2021-12-27	not yet calculated	CVE-2020-20946 MISC MISC
qibosoft -- qibosoft	An issue in /admin/index.php?lfj=mysql&action=del of Qibosoft v7 allows attackers to arbitrarily delete files.	2021-12-27	not yet calculated	CVE-2020-20944 MISC MISC
qt_svg-- qt_svg	Qt SVG in Qt 5.0.0 through 5.15.2 and 6.0.0 through 6.2.1 has an out-of-bounds write in QtPrivate::QCommonArrayOps<QPainterPath::Element>::growAppend (called from QPainterPath::addPath and QPathClipper::intersect).	2022-01-01	not yet calculated	CVE-2021-45930 MISC MISC MISC MISC MISC MISC
quectel -- uc20	Quectel UC20 UMTS/HSPA+ UC20 6.3.14 is affected by a Cross Site Scripting (XSS) vulnerability.	2021-12-30	not yet calculated	CVE-2021-45815 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
requarks -- wiki.js	In Requarks wiki.js, versions 2.0.0-beta.147 to 2.5.255 are affected by Stored XSS vulnerability, where a low privileged (editor) user can upload a SVG file that contains malicious JavaScript while uploading assets in the page. That will send the JWT tokens to the attacker's server and will lead to account takeover when accessed by the victim.	2021-12-29	not yet calculated	CVE-2021-25993 MISC MISC
requarks -- wiki.js	Wiki.js is a wiki app built on Node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through non-image file uploads for file types that can be viewed directly inline in the browser. By creating a malicious file which can execute inline JS when viewed in the browser (e.g. XML files), a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the file is viewed directly by other users. The file must be opened directly by the user and will not trigger directly in a normal Wiki.js page. A patch in version 2.5.264 fixes this vulnerability by adding an optional (enabled by default) force download flag to all non-image file types, preventing the file from being viewed inline in the browser. As a workaround, disable file upload for all non-trusted users. --- Thanks to @Haxatron for reporting this vulnerability. Initially reported via https://huntr.dev/bounties/266bff09-00d9-43ca-a4bb-bb540642811f/	2021-12-27	not yet calculated	CVE-2021-43856 CONFIRM MISC MISC
requarks -- wiki.js	Wiki.js is a wiki app built on node.js. Wiki.js 2.5.263 and earlier is vulnerable to stored cross-site scripting through a SVG file upload made via a custom request with a fake MIME type. By creating a crafted SVG file, a malicious Wiki.js user may stage a stored cross-site scripting attack. This allows the attacker to execute malicious JavaScript when the SVG is viewed directly by other users. Scripts do not execute when loaded inside a page via normal `<img>` tags. The malicious SVG can only be uploaded by crafting a custom request to the server with a fake MIME type. A patch in version 2.5.264 fixes this vulnerability by adding an additional file extension verification check to the optional (enabled by default) SVG sanitization step to all file uploads that match the SVG mime type. As a workaround, disable file upload for all non-trusted users.	2021-12-27	not yet calculated	CVE-2021-43855 MISC CONFIRM MISC
ruby -- ruby	CGI::Cookie.parse in Ruby through 2.6.8 mishandles security prefixes in cookie names. This also affects the CGI gem through 0.3.0 for Ruby.	2022-01-01	not yet calculated	CVE-2021-41819 MISC CONFIRM
ruby -- ruby	Date.parse in the date gem through 3.2.0 for Ruby allows ReDoS (regular expression Denial of Service) via a long string. The fixed versions are 3.2.1, 3.1.2, 3.0.2, and 2.0.1.	2022-01-01	not yet calculated	CVE-2021-41817 MISC CONFIRM
rust -- rust	An issue was discovered in the binjs_io crate through 2021-01-03 for Rust. The Read method may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45683 MISC MISC
rust -- rust	An issue was discovered in the csv-sniffer crate through 2021-01-05 for Rust. preamble_skipcount may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45686 MISC MISC
rust -- rust	An issue was discovered in the columnar crate through 2021-01-07 for Rust. ColumnarReadExt::read_typed_vec may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45685 MISC MISC
rust -- rust	An issue was discovered in the flumedb crate through 2021-01-07 for Rust. read_entry may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45684 MISC MISC
rust -- rust	An issue was discovered in the vec-const crate before 2.0.0 for Rust. It tries to construct a Vec from a pointer to a const slice, leading to memory corruption.	2021-12-27	not yet calculated	CVE-2021-45680 MISC MISC
rust -- rust	An issue was discovered in the nanorand crate before 0.6.1 for Rust. There can be multiple mutable references to the same object because the TlsWyRand Deref implementation dereferences a raw pointer.	2021-12-27	not yet calculated	CVE-2021-45705 MISC MISC
rust -- rust	An issue was discovered in the bronzedb-protocol crate through 2021-01-03 for Rust. ReadKVExt may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45682 MISC MISC
rust -- rust	An issue was discovered in the metrics-util crate before 0.7.0 for Rust. There is a data race and memory corruption because AtomicBucket<T> unconditionally implements the Send and Sync traits.	2021-12-27	not yet calculated	CVE-2021-45704 MISC MISC
rust -- rust	An issue was discovered in the ckb crate before 0.40.0 for Rust. Remote attackers may be able to conduct a 51% attack against the Nervos CKB blockchain by triggering an inability to allocate memory for the misbehavior HashMap.	2021-12-27	not yet calculated	CVE-2021-45699 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rust -- rust	An issue was discovered in the derive-com-impl crate before 0.1.2 for Rust. An invalid reference (and memory corruption) can occur because AddRef might not be called before returning a pointer.	2021-12-27	not yet calculated	CVE-2021-45681 MISC MISC
rust -- rust	An issue was discovered in the raw-cpuid crate before 9.1.1 for Rust. If the serialize feature is used (which is not the the default), a Deserialize operation may lack sufficient validation, leading to memory corruption or a panic.	2021-12-27	not yet calculated	CVE-2021-45687 MISC MISC
rust -- rust	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_string may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45691 MISC MISC
rust -- rust	An issue was discovered in the gfx-auxil crate through 2021-01-07 for Rust. gfx_auxil::read_spirv may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45689 MISC MISC
rust -- rust	An issue was discovered in the ckb crate before 0.40.0 for Rust. Attackers can cause a denial of service (Nervos CKB blockchain node crash) via a dead call that is used as a DepGroup.	2021-12-27	not yet calculated	CVE-2021-45700 MISC MISC
rust -- rust	An issue was discovered in the abomonation crate through 2021-10-17 for Rust. Because transmute operations are insufficiently constrained, there can be an information leak or ASLR bypass.	2021-12-27	not yet calculated	CVE-2021-45708 MISC MISC
rust -- rust	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_binary may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45690 MISC MISC
rust -- rust	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_extension_others may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45692 MISC MISC
rust -- rust	An issue was discovered in the messagepack-rs crate through 2021-01-26 for Rust. deserialize_string_primitive may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45693 MISC MISC
rust -- rust	An issue was discovered in the rdiff crate through 2021-02-03 for Rust. Window may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45694 MISC MISC
rust -- rust	An issue was discovered in the mopa crate through 2021-06-01 for Rust. It incorrectly relies on Trait memory layout, possibly leading to future occurrences of arbitrary code execution or ASLR bypass.	2021-12-27	not yet calculated	CVE-2021-45695 MISC MISC
rust -- rust	An issue was discovered in the sha2 crate 0.9.7 before 0.9.8 for Rust. Hashes of long messages may be incorrect when the AVX2-accelerated backend is used.	2021-12-27	not yet calculated	CVE-2021-45696 MISC MISC
rust -- rust	An issue was discovered in the molecule crate before 0.7.2 for Rust. A FixVec partial read has an incorrect result.	2021-12-27	not yet calculated	CVE-2021-45697 MISC MISC
rust -- rust	An issue was discovered in the ckb crate before 0.40.0 for Rust. A get_block_template RPC call may fail in situations where it is supposed to select a Nervos CKB blockchain transaction with a higher fee rate than another transaction.	2021-12-27	not yet calculated	CVE-2021-45698 MISC MISC
rust -- rust	An issue was discovered in the ash crate before 0.33.1 for Rust. util::read_spv may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45688 MISC MISC
rust -- rust	An issue was discovered in the acc_reader crate through 2020-12-27 for Rust. read_up_to may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2020-36513 MISC MISC
rust -- rust	An issue was discovered in the zeroize_derive crate before 1.1.1 for Rust. Dropped memory is not zeroed out for an enum.	2021-12-27	not yet calculated	CVE-2021-45706 MISC MISC
rust -- rust	An issue was discovered in the simple_asn1 crate 0.6.0 before 0.6.1 for Rust. There is a panic if UTCTime data, supplied by a remote attacker, has a second character greater than 0x7f.	2021-12-27	not yet calculated	CVE-2021-45711 MISC MISC
rust -- rust	An issue was discovered in the pnet crate before 0.27.2 for Rust. There is a segmentation fault (upon attempted dereference of an uninitialized descriptor) because of an erroneous IcmpTransportChannelIterator compiler optimization.	2021-12-27	not yet calculated	CVE-2019-25054 MISC MISC
rust -- rust	An issue was discovered in the buffoon crate through 2020-12-31 for Rust. InputStream::read_exact may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2020-36512 MISC MISC
rust -- rust	An issue was discovered in the bite crate through 2020-12-31 for Rust. read::BiteReadExpandedExt::read_framed_max may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2020-36511 MISC MISC
rust -- rust	An issue was discovered in the libpulse-binding crate before 2.6.0 for Rust. It mishandles a panic that crosses a Foreign Function Interface (FFI) boundary.	2021-12-27	not yet calculated	CVE-2019-25055 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rust -- rust	An issue was discovered in the crypto2 crate through 2021-10-08 for Rust. During Chacha20 encryption and decryption, an unaligned read of a u32 may occur.	2021-12-27	not yet calculated	CVE-2021-45709 MISC MISC
rust -- rust	An issue was discovered in the libpulse-binding crate before 1.2.1 for Rust. get_context can cause a use-after-free.	2021-12-27	not yet calculated	CVE-2018-25028 MISC MISC
rust -- rust	An issue was discovered in the libpulse-binding crate before 1.2.1 for Rust. get_format_info can cause a use-after-free.	2021-12-27	not yet calculated	CVE-2018-25027 MISC MISC
rust -- rust	An issue was discovered in the tokio crate before 1.8.4, and 1.9.x through 1.13.x before 1.13.1, for Rust. In certain circumstances involving a closed oneshot channel, there is a data race and memory corruption.	2021-12-27	not yet calculated	CVE-2021-45710 MISC MISC
rust -- rust	An issue was discovered in the acc_reader crate through 2020-12-27 for Rust. fill_buf may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2020-36514 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_window_function has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45715 MISC MISC
rust -- rust	An issue was discovered in the nix crate before 0.20.2, 0.21.x before 0.21.2, and 0.22.x before 0.22.2 for Rust. unistd::getgrouplist has an out-of-bounds write if a user is in more than 16 /etc/groups groups.	2021-12-27	not yet calculated	CVE-2021-45707 MISC MISC
rust -- rust	An issue was discovered in the tremor-script crate before 0.11.6 for Rust. A merge operation may result in a use-after-free.	2021-12-27	not yet calculated	CVE-2021-45702 MISC MISC
rust -- rust	An issue was discovered in the tremor-script crate before 0.11.6 for Rust. A patch operation may result in a use-after-free.	2021-12-27	not yet calculated	CVE-2021-45701 MISC MISC
rust -- rust	An issue was discovered in the lru crate before 0.7.1 for Rust. The iterators have a use-after-free, as demonstrated by an access after a pop operation.	2021-12-26	not yet calculated	CVE-2021-45720 MISC MISC
rust -- rust	An issue was discovered in the tectonic_xdv crate before 0.1.12 for Rust. XdvParser::<T>::process may read from uninitialized memory locations.	2021-12-27	not yet calculated	CVE-2021-45703 MISC MISC
rust -- rust	An issue was discovered in the rust-embed crate before 6.3.0 for Rust. A ../ directory traversal can sometimes occur in debug mode.	2021-12-26	not yet calculated	CVE-2021-45712 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_scalar_function has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45713 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_aggregate_function has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45714 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. create_collation has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45716 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. commit_hook has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45717 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. rollback_hook has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45718 MISC MISC
rust -- rust	An issue was discovered in the rusqlite crate 0.25.x before 0.25.4 and 0.26.x before 0.26.2 for Rust. update_hook has a use-after-free.	2021-12-26	not yet calculated	CVE-2021-45719 MISC MISC
safari -- montage	Reflected Cross Site Scripting (XSS) in SAFARI Montage versions 8.3 and 8.5 allows remote attackers to execute JavaScript codes.	2021-12-28	not yet calculated	CVE-2021-45425 MISC MISC
safari_montage -- safari_montage	SAFARI Montage 8.7.32 is affected by a CRLF injection vulnerability which can lead to can lead to HTTP response splitting.	2021-12-30	not yet calculated	CVE-2021-45818 MISC
servo -- rust-smallvec	An issue was discovered in the smallvec crate before 0.6.13 for Rust. It can create an uninitialized value of any type, including a reference type.	2021-12-27	not yet calculated	CVE-2018-25023 MISC MISC
showdoc -- showdoc	showdoc is vulnerable to Cross-Site Request Forgery (CSRF)	2021-12-26	not yet calculated	CVE-2021-4168 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
slican -- webcti	SLICAN WebCTI 1.01 2015 is affected by a Cross Site Scripting (XSS) vulnerability. The attacker can steal the user's session by injecting malicious JavaScript codes which leads to Session Hijacking and cause user's credentials theft.	2021-12-28	not yet calculated	CVE-2021-45813 MISC
snapdragon -- qnap_devices	A stack buffer overflow vulnerability has been reported to affect QNAP NAS running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. We have already fixed this vulnerability in the following versions of Surveillance Station: QTS 5.0.0 (64 bit): Surveillance Station 5.2.0.4.2 (2021/10/26) and later QTS 5.0.0 (32 bit): Surveillance Station 5.2.0.3.2 (2021/10/26) and later QTS 4.3.6 (64 bit): Surveillance Station 5.1.5.4.6 (2021/10/26) and later QTS 4.3.6 (32 bit): Surveillance Station 5.1.5.3.6 (2021/10/26) and later QTS 4.3.3: Surveillance Station 5.1.5.3.6 (2021/10/26) and later	2021-12-29	not yet calculated	CVE-2021-38687 CONFIRM
snapdragon -- qnap_devices	A cross-site scripting (XSS) vulnerability has been reported to affect QNAP device running Kazoo Server. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions of Kazoo Server: Kazoo Server 4.11.20 and later	2021-12-29	not yet calculated	CVE-2021-38680 CONFIRM
solarwinds -- web_help_desk	Hard coded credentials discovered in SolarWinds Web Help Desk product. Through these credentials, the attacker with local access to the Web Help Desk host machine allows to execute arbitrary HQL queries against the database and leverage the vulnerability to steal the password hashes of the users or insert arbitrary data into the database.	2021-12-27	not yet calculated	CVE-2021-35232 MISC MISC
sourcecodester -- online_enrollment_management_system	https://www.sourcecodester.com/ Online Enrollment Management System in PHP and PayPal Free Source Code 1.0 is affected by: Incorrect Access Control. The impact is: gain privileges (remote).	2021-12-28	not yet calculated	CVE-2021-40579 MISC MISC
stormshield -- stormshield_network_security	An issue was discovered in Stormshield Network Security (SNS) 4.2.2 through 4.2.7 (fixed in 4.2.8). Under a specific update-migration scenario, the first SSH password change does not properly clear the old password.	2021-12-29	not yet calculated	CVE-2021-45885 CONFIRM MISC
suitecrm -- suitecrm	A persistent cross-site scripting (XSS) issue in the web interface of SuiteCRM before 7.10.35, and 7.11.x and 7.12.x before 7.12.2, allows a remote attacker to introduce arbitrary JavaScript via attachments upload, a different vulnerability than CVE-2021-39267 and CVE-2021-39268.	2021-12-28	not yet calculated	CVE-2021-45903 MISC MISC MISC
superantispyware -- superantispyware	SUPERAntispyware v8.0.0.1050 was discovered to contain an issue in the component saskutil64.sys. This issue allows attackers to arbitrarily write data to the device via IOCTL 0x9C402140.	2021-12-28	not yet calculated	CVE-2020-22061 MISC
tenable -- d-link	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 use default hard-coded credentials, which can allow a remote attacker to gain administrative access to the zebra or ripd those services. Both are running with root privileges on the router (i.e., as the "admin" user, UID 0).	2021-12-30	not yet calculated	CVE-2021-20132 MISC
tenable -- d-link	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 are affected by an absolute path traversal vulnerability that allows a remote, authenticated attacker to set the "message of the day" banner to any file on the system, allowing them to read all or some of the contents of those files. Such sensitive information as hashed credentials, hardcoded plaintext passwords for other services, configuration files, and private keys can be disclosed in this fashion. Improper handling of filenames that identify virtual resources, such as "/dev/urandom" allows an attacker to effect a denial of service attack against the command line interfaces of the Quagga services (zebra and ripd).	2021-12-30	not yet calculated	CVE-2021-20133 MISC
tenable -- trendnet_ac2600	It is possible for an unauthenticated, malicious user to force the device to reboot due to a hidden administrative command.	2021-12-30	not yet calculated	CVE-2021-20157 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 lacks proper authentication to the bittorrent functionality. If enabled, anyone is able to visit and modify settings and files via the Bittorent web client by visiting: http://192.168.10.1:9091/transmission/web/	2021-12-30	not yet calculated	CVE-2021-20152 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 improperly discloses information via redirection from the setup wizard. Authentication can be bypassed and a user may view information as Admin by manually browsing to the setup wizard and forcing it to redirect to the desired page.	2021-12-30	not yet calculated	CVE-2021-20150 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 does not have sufficient access controls for the WAN interface. The default iptables ruleset for governing access to services on the device only apply to IPv4. All services running on the devices are accessible via the WAN interface via IPv6 by default.	2021-12-30	not yet calculated	CVE-2021-20149 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- trendnet_ac2600	Quagga Services on D-Link DIR-2640 less than or equal to version 1.11B02 are affected by an absolute path traversal vulnerability that allows a remote, authenticated attacker to set an arbitrary file on the router's filesystem as the log file used by either Quagga service (zebra or ripd). Subsequent log messages will be appended to the file, prefixed by a timestamp and some logging metadata. Remote code execution can be achieved by using this vulnerability to append to a shell script on the router's filesystem, and then awaiting or triggering the execution of that script. A remote, unauthenticated root shell can easily be obtained on the device in this fashion.	2021-12-30	not yet calculated	CVE-2021-20134 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 does not properly implement csrf protections. Most pages lack proper usage of CSRF protections or mitigations. Additionally, pages that do make use of CSRF tokens are trivially bypassable as the server does not appear to validate them properly (i.e. re-using an old token or finding the token thru some other method is possible).	2021-12-30	not yet calculated	CVE-2021-20165 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 improperly discloses credentials for the smb functionality of the device. Usernames and passwords for all smb users are revealed in plaintext on the smbserver.asp page.	2021-12-30	not yet calculated	CVE-2021-20164 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 leaks information via the ftp web page. Usernames and passwords for all ftp users are revealed in plaintext on the ftpserver.asp page.	2021-12-30	not yet calculated	CVE-2021-20163 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an improper access control configuration that could allow for a malicious firmware update. It is possible to manually install firmware that may be malicious in nature as there does not appear to be any signature validation done to determine if it is from a known and trusted source. This includes firmware updates that are done via the automated "check for updates" in the admin interface. If an attacker is able to masquerade as the update server, the device will not verify that the firmware updates downloaded are legitimate.	2021-12-30	not yet calculated	CVE-2021-20156 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 makes use of hardcoded credentials. It is possible to backup and restore device configurations via the management web interface. These devices are encrypted using a hardcoded password of "12345678".	2021-12-30	not yet calculated	CVE-2021-20155 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a command injection vulnerability in the smb functionality of the device. The username parameter used when configuring smb functionality for the device is vulnerable to command injection as root.	2021-12-30	not yet calculated	CVE-2021-20160 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a symlink vulnerability in the bittorrent functionality. If enabled, the bittorrent functionality is vulnerable to a symlink attack that could lead to remote code execution on the device. If an end user inserts a flash drive with a malicious symlink on it that the bittorrent client can write downloads to, then a user is able to download arbitrary files to any desired location on the devices filesystem, which could lead to remote code execution. Example directories vulnerable to this include "config", "downloads", and "torrents", though it should be noted that "downloads" is the only vector that allows for arbitrary files to be downloaded to arbitrary locations.	2021-12-30	not yet calculated	CVE-2021-20153 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an security flaw in the web interface. HTTPS is not enabled on the device by default. This results in cleartext transmission of sensitive information such as passwords.	2021-12-30	not yet calculated	CVE-2021-20154 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains a flaw in the session management for the device. The router's management software manages web sessions based on IP address rather than verifying client cookies/session tokens/etc. This allows an attacker (whether from a different computer, different web browser on the same machine, etc.) to take over an existing session. This does require the attacker to be able to spoof or take over original IP address of the original user's session.	2021-12-30	not yet calculated	CVE-2021-20151 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 does not have sufficient protections for the UART functionality. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection. No username or password is required and the user is given a root shell with full control of the device.	2021-12-30	not yet calculated	CVE-2021-20161 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 contains an authentication bypass vulnerability. It is possible for an unauthenticated, malicous actor to force the change of the admin password due to a hidden administrative command.	2021-12-30	not yet calculated	CVE-2021-20158 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 is vulnerable to command injection. The system log functionality of the firmware allows for command injection as root by supplying a malformed parameter.	2021-12-30	not yet calculated	CVE-2021-20159 MISC
tenable -- trendnet_ac2600	Trendnet AC2600 TEW-827DRU version 2.08B01 stores credentials in plaintext. Usernames and passwords are stored in plaintext in the config files on the device. For example, /etc/config/cameo contains the admin password in plaintext.	2021-12-30	not yet calculated	CVE-2021-20162 MISC
ultrajson -- ultrajson	UltraJSON (aka ujson) 4.0.2 through 5.0.0 has a stack-based buffer overflow in Buffer_AppendIndentUnchecked (called from encode).	2022-01-01	not yet calculated	CVE-2021-45958 MISC MISC
unicorn -- engine	An issue was discovered in split_region in uc.c in Unicorn Engine before 2.0.0-rc5. It allows local attackers to escape the sandbox. An attacker must first obtain the ability to execute crafted code in the target sandbox in order to exploit this vulnerability. The specific flaw exists within the virtual memory manager. The issue results from the faulty comparison of GVA and GPA while calling uc_mem_map_ptr to free part of a claimed memory block. An attacker can leverage this vulnerability to escape the sandbox and execute arbitrary code on the host machine.	2021-12-26	not yet calculated	CVE-2021-44078 MISC CONFIRM MISC MISC MISC
uwebsockets -- uwebsockets	uWebSockets 19.0.0 through 20.8.0 has an out-of-bounds write in std::__1::pair<unsigned int, void*> uWS::HttpParser::fenceAndConsumePostPadded<0 (called from uWS::HttpParser::consumePostPadded and std::__1::__function::__func<LLVMFuzzerTestOneInput::$_0, std::__1::allocator<LL).	2022-01-01	not yet calculated	CVE-2021-45945 MISC MISC MISC
vim -- vim	vim is vulnerable to Use After Free	2021-12-29	not yet calculated	CVE-2021-4187 MISC CONFIRM
vim -- vim	vim is vulnerable to Out-of-bounds Read	2021-12-25	not yet calculated	CVE-2021-4166 CONFIRM MISC
vim -- vim	vim is vulnerable to Use After Free	2021-12-31	not yet calculated	CVE-2021-4192 CONFIRM MISC
vim -- vim	vim is vulnerable to Use After Free	2021-12-27	not yet calculated	CVE-2021-4173 CONFIRM MISC
vim -- vim	vim is vulnerable to Out-of-bounds Read	2021-12-31	not yet calculated	CVE-2021-4193 MISC CONFIRM
wasm3 -- wasm3	Wasm3 0.5.0 has an out-of-bounds write in Runtime_Release (called from EvaluateExpression and InitDataSegments).	2022-01-01	not yet calculated	CVE-2021-45947 MISC MISC
wasm3 -- wasm3	Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from CompileElseBlock and Compile_If).	2022-01-01	not yet calculated	CVE-2021-45929 MISC MISC
wasm3 -- wasm3	Wasm3 0.5.0 has an out-of-bounds write in CompileBlock (called from Compile_LoopOrBlock and CompileBlockStatements).	2022-01-01	not yet calculated	CVE-2021-45946 MISC MISC
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::Frame::page, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45483 MISC
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is a use-after-free in WebCore::ContainerNode::firstChild, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45482 MISC
webkitgtk -- webkitgtk	In WebKitGTK before 2.32.4, there is incorrect memory allocation in WebCore::ImageBufferCairoImageSurfaceBackend::create, leading to a segmentation violation and application crash, a different vulnerability than CVE-2021-30889.	2021-12-25	not yet calculated	CVE-2021-45481 MISC
wireshark -- wireshark	Infinite loop in the BitTorrent DHT dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4184 MISC CONFIRM MISC
wireshark -- wireshark	Crash in the pcapng file parser in Wireshark 3.6.0 allows denial of service via crafted capture file	2021-12-30	not yet calculated	CVE-2021-4183 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wireshark -- wireshark	Crash in the Sysdig Event dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4181 CONFIRM MISC MISC
wireshark -- wireshark	Infinite loop in the RTMPT dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4185 MISC CONFIRM MISC
wireshark -- wireshark	Crash in the Gryphon dissector in Wireshark 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4186 CONFIRM MISC MISC
wireshark -- wireshark	Large loop in the Kafka dissector in Wireshark 3.6.0 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4190 CONFIRM MISC MISC
wireshark -- wireshark	Crash in the RFC 7468 dissector in Wireshark 3.6.0 and 3.4.0 to 3.4.10 allows denial of service via packet injection or crafted capture file	2021-12-30	not yet calculated	CVE-2021-4182 MISC CONFIRM MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttDecode_Disconnect (called from MqttClient_DecodePacket and MqttClient_WaitType).	2022-01-01	not yet calculated	CVE-2021-45936 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Unsubscribe).	2022-01-01	not yet calculated	CVE-2021-45938 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (8 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).	2022-01-01	not yet calculated	CVE-2021-45933 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_HandlePacket and MqttClient_WaitType).	2022-01-01	not yet calculated	CVE-2021-45934 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Connect).	2022-01-01	not yet calculated	CVE-2021-45937 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow (4 bytes) in MqttDecode_Publish (called from MqttClient_DecodePacket and MqttClient_HandlePacket).	2022-01-01	not yet calculated	CVE-2021-45932 MISC MISC MISC
wolfssl -- wolfssl	wolfSSL wolfMQTT 1.9 has a heap-based buffer overflow in MqttClient_DecodePacket (called from MqttClient_WaitType and MqttClient_Subscribe).	2022-01-01	not yet calculated	CVE-2021-45939 MISC MISC MISC
wordpress -- wordpress	The Smart Floating / Sticky Buttons WordPress plugin before 2.5.5 does not sanitise and escape some parameter before outputting them in attributes and page, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-12-27	not yet calculated	CVE-2021-24992 MISC
wordpress -- wordpress	The Simple JWT Login WordPress plugin before 3.3.0 can be used to create new WordPress user accounts with a randomly generated password. The password is generated using the str_shuffle PHP function that "does not generate cryptographically secure values, and should not be used for cryptographic purposes" according to PHP's documentation.	2021-12-27	not yet calculated	CVE-2021-24998 MISC CONFIRM
wordpress -- wordpress	The Paid Memberships Pro WordPress plugin before 2.6.6 does not escape the s parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	2021-12-27	not yet calculated	CVE-2021-24979 CONFIRM MISC
wordpress -- wordpress	The Rich Reviews by Starfish WordPress plugin before 1.9.6 does not properly validate the orderby GET parameter of the pending reviews page before using it in a SQL statement, leading to an authenticated SQL injection issue	2021-12-27	not yet calculated	CVE-2021-24753 MISC CONFIRM
wordpress -- wordpress	The Tickera WordPress plugin before 3.4.8.3 does not properly sanitise and escape the Name fields of booked Events before outputting them in the Orders admin dashboard, which could allow unauthenticated users to perform Cross-Site Scripting attacks against admins.	2021-12-27	not yet calculated	CVE-2021-24797 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The WordPress Download Manager WordPress plugin before 3.2.22 does not sanitise and escape Template data before outputting it in various pages (such as admin dashboard and frontend). Due to the lack of authorisation and CSRF checks in the wpdm_save_template AJAX action, any authenticated users such as subscriber is able to call it and perform Cross-Site Scripting attacks	2021-12-27	not yet calculated	CVE-2021-24969 MISC
wordpress -- wordpress	The Typebot | Build beautiful conversational forms WordPress plugin before 1.4.3 does not sanitise and escape the Publish ID setting, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-12-27	not yet calculated	CVE-2021-24902 MISC
wordpress -- wordpress	The Contact Form & Lead Form Elementor Builder WordPress plugin before 1.6.4 does not sanitise and escape some lead values, which could allow unauthenticated users to perform Cross-Site Scripting attacks against logged in admin viewing the inserted Leads	2021-12-27	not yet calculated	CVE-2021-24967 MISC
wordpress -- wordpress	The Gwolle Guestbook WordPress plugin before 4.2.0 does not sanitise and escape the gwolle_gb_user_email parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue in an admin page	2021-12-27	not yet calculated	CVE-2021-24980 MISC
wordpress -- wordpress	The WP Guppy WordPress plugin before 1.3 does not have any authorisation in some of the REST API endpoints, allowing any user to call them and could lead to sensitive information disclosure, such as usernames and chats between users, as well as be able to send messages as an arbitrary user	2021-12-27	not yet calculated	CVE-2021-24997 MISC MISC
wordpress -- wordpress	The WPFront User Role Editor WordPress plugin before 3.2.1.11184 does not sanitise and escape the changes-saved parameter before outputting it back in the admin dashboard, leading to a Reflected Cross-Site Scripting	2021-12-27	not yet calculated	CVE-2021-24984 MISC
wordpress -- wordpress	The WP RSS Aggregator WordPress plugin before 4.19.3 does not sanitise and escape data before outputting it in the System Info admin dashboard, which could lead to a Stored XSS issue due to the wprss_dismiss_addon_notice AJAX action missing authorisation and CSRF checks, allowing any authenticated users, such as subscriber to call it and set a malicious payload in the addon parameter.	2021-12-27	not yet calculated	CVE-2021-24988 MISC
wowsoft -- printchaser_activex	Printchaser v2.2021.804.1 and earlier versions contain a vulnerability, which could allow remote attacker to download and execute remote file by setting the argument, variable in the activeX module. This can be leveraged for code execution.	2021-12-28	not yet calculated	CVE-2020-7883 MISC
yappli -- yappli	Yappli is an application development platform which provides the function to access a requested URL using Custom URL Scheme. When Android apps are developed with Yappli versions since v7.3.6 and prior to v9.30.0, they are vulnerable to improper authorization in Custom URL Scheme handler, and may be directed to unintended sites via a specially crafted URL.	2021-12-28	not yet calculated	CVE-2021-20873 MISC MISC
zte -- bigvideo_analysis	ZTE BigVideo Analysis product has a privilege escalation vulnerability. Due to improper management of the timed task modification privilege, an attacker with ordinary user permissions could exploit this vulnerability to gain unauthorized access.	2021-12-27	not yet calculated	CVE-2021-21750 MISC
zte -- bigvideo_analysis	ZTE BigVideo analysis product has an input verification vulnerability. Due to the inconsistency between the front and back verifications when configuring the large screen page, an attacker with high privileges could exploit this vulnerability to tamper with the URL and cause service exception.	2021-12-27	not yet calculated	CVE-2021-21751 MISC
zyxel -- gs1900_firmware	A vulnerability in the 'libsal.so' of the Zyxel GS1900 series firmware version 2.60 could allow an authenticated local user to execute arbitrary OS commands via a crafted function call.	2021-12-28	not yet calculated	CVE-2021-35032 CONFIRM
zyxel -- multiple_products	A vulnerability in the TFTP client of Zyxel GS1900 series firmware, XGS1210 series firmware, and XGS1250 series firmware, which could allow an authenticated LAN user to execute arbitrary OS commands via the GUI of the vulnerable device.	2021-12-28	not yet calculated	CVE-2021-35031 CONFIRM
zyxel -- nbg6604_firmware	A cleartext storage of sensitive information vulnerability in the Zyxel NBG6604 firmware could allow a remote, authenticated attacker to obtain sensitive information from the configuration file.	2021-12-29	not yet calculated	CVE-2021-35035 CONFIRM
zyxel -- nbg6604_firmware	An insufficient session expiration vulnerability in the CGI program of the Zyxel NBG6604 firmware could allow a remote attacker to access the device if the correct token can be intercepted.	2021-12-29	not yet calculated	CVE-2021-35034 CONFIRM

Back to top